Impossible Differential Cryptanalysis of Reduced-Round SKINNY

Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef

Concordia Institute for Information Systems Engineering,
Concordia University, Montréal, Quebéc, Canada

Abstract. SKINNY is a new lightweight tweakable block cipher family proposed by Beierle *et al*. in CRYPTO 2016. SKINNY-n-t is a block cipher with n-bit state and t-bit tweakey (key and tweak). It is designed to compete with the recent NSA SIMON block cipher. In this paper, we present impossible differential attacks against reduced-round versions of all the 6 SKINNY's variants, namely, SKINNY-n-n, SKINNY-n-$2n$ and SKINNY-n-$3n$ ($n = 64$ or $n = 128$) in the single-tweakey model. More precisely, we present impossible differential attacks against 18, 20 and 22 rounds of SKINNY-n-n, SKINNY-n-$2n$ and SKINNY-n-$3n$ ($n = 64$ or $n = 128$), respectively. These attacks are based on the same 11-round impossible differential distinguisher. To the best of our knowledge, these are the best attacks against these 6 variants of the cipher in the single-tweakey model.

Keywords: Cryptanalysis, Impossible differential attacks, Tweakable, Block ciphers, SKINNY.

1 Introduction

SKINNY [4] is a Substitution Permutation Network (SPN) family of lightweight block ciphers that was proposed in CRYPTO 2016 by Beierle *et al*. These family of ciphers inherit the new design trend of having an SPN cipher with non optimal internal components. More precisely, each round function employs a compact S-box, a new very sparse diffusion layer, and a new very light key schedule. The arrangement of these components in SKINNY guarantees strong security. Indeed, the designers of SKINNY using Mixed Integer Linear Programming (MILP) provide high security bounds against differential/linear attacks for all the SKINNY versions in the single-key and related-key models. Compared to SIMON [1], SKINNY provides security guarantee against the best differential/linear characteristics for a much lower proportion of its total number of rounds in the single-key model. While all the versions of SIMON have no bounds against the differential/linear attacks in the related-key model, SKINNY has strong bounds.

SKINNY is the first block cipher family that has better performance than SIMON for round-based ASIC implementations. Moreover, using the serial ASIC it requires a very small area. Therefore, SKINNY is an integrated work of lightweight block ciphers design that offer high security guarantee. In addition to the serial implementation, the designers of SKINNY exhibit that its ASIC threshold implementations is very favorable to AES-128 threshold implementations [7]. Compared to the software implementations of all the lightweight block ciphers except SIMON (in cases where the key schedule is performed only once), SKINNY has the most efficient performance. But according to [5], the key schedule has to be performed every time in practical applications. Therefore, in these scenarios SKINNY implementation is equivalent to SIMON. Moreover, SKINNY is competitive for most platforms since it has the smallest total number of AND/NOR/XOR gates. In addition, SKINNY has the advantage that the encryption and decryption algorithms are almost exact.

Compared to SIMON, SKINNY has the advantage of being tweakable. This advantage is useful in the leakage resilient implementations and allows SKINNY to be employed into a higher level of operating modes such as SCT [11]. Moreover, the designers of SKINNY generalized the STK construction [9] in order to provide compact implementation while the existence of the tweakey with providing high level of security.

The designers of SKINNY [2] presented 16-round attacks against SKINNY-n-t ($n = 64$ or $n = 128$) utilizing 11-round impossible distinguisher, that will be utilized in our attacks against all the 6 variants of SKINNY cipher. Moreover, the designers of SKINNY announced a competition [3] against two variants of SKINNY, namely, SKINNY-64-128 and SKINNY-128-128. In this competition, the authors indicate that the best known attack against SKINNY-64-128 is 18 rounds.

In this paper, we present impossible differential attacks against all the 6 variants of SKINNY, namely, SKINNY-n-t, SKINNY-n-$2t$ and SKINNY-n-$3t$ ($n = 64$ or $n = 128$). All of these attacks utilize the same impossible differential distinguisher that is used by the designers of SKINNY to launch 16-round attacks against SKINNY-n-t ($n = 64$ or $n = 128$). We exploited the fact that the tweakey addition are only performed on the first two rows of the state along with the MixColumn operation properties and the tweakey schedule relations to extend this distinguisher by 7, 9, 11 rounds to launch key recovery attacks in the single-tweakey model against 18, 20, 22 rounds of SKINNY-n-t, SKINNY-n-$2t$ and SKINNY-n-$3t$ ($n = 64$ or $n = 128$), respectively. More specifically, we extend this impossible differential distinguisher by 3, 3 and 3 rounds above it and 4, 6 and 8 rounds below it to launch 18, 20 and 22 rounds attacks against SKINNY-n-t, SKINNY-n-$2t$ and SKINNY-n-$3t$ ($n = 64$ or $n = 128$), respectively. The time, data and memory complexities of our attacks are presented in Table 1.

Table 1. The time, data and memory complexities of our 4 attacks.

Block cipher version	# of rounds	Time	Data	Memory
SKINNY-64-64	18	$2^{57.1}$	$2^{47.52}$	$2^{58.52}$
SKINNY-128-128	18	$2^{116.94}$	$2^{92.42}$	$2^{115.42}$
SKINNY-64-128	20	$2^{121.08}$	$2^{47.69}$	$2^{74.69}$
SKINNY-128-256	20	$2^{245.72}$	$2^{92.1}$	$2^{147.1}$
SKINNY-64-192	22	$2^{183.97}$	$2^{47.84}$	$2^{74.84}$
SKINNY-128-384	22	$2^{373.48}$	$2^{92.22}$	$2^{147.22}$

The rest of the paper is organized as follows. Section 2 provides the notations used throughout the paper and a brief description of SKINNY . In section 3, we present the impossible differential distinguisher used in our attacks. The details of our attacks are presented in sections 4, 5 and 6, respectively. Finally, the paper is concluded in section 7.

2 Specifications of SKINNY

The following notations are used throughout the rest of the paper:

- TK_i: The round tweakey used in round i.
- ETK_i: The equivalent round tweakey used in round i.
- x_i: The input to the SubCells (SC) operation at round i.
- y_i: The input to the AddRoundConstantTweakey (AK) operation at round i.
- $y_i^{'}$: The input to the AddRoundConstantEquivlantTweakey (AEK) operation at round i.
- z_i: The input to the ShiftRows (SR) operation at round i.
- w_i: The input to the MixColumns (MC) operation at round i.
- $x_i[j]$: The j^{th} cell of x_i, where $0 \le j < 16$.
- $x_i[j \cdots l]$: The cells from j to l of x_i, where $j < l$.
- $x_i[j, l]$: The cells j and l of x_i.
- $x_i[j][k]$: The k^{th} bit of the j^{th} cell of x_i.
- $x_i[j]\{k, l, m\}$: The XOR of bits k, l, m of cell j of x_i.
- $x_i[col : j]$: The four cells in column j, e.g., $x_i[col : 0] = x_i[0, 4, 8, 12]$.

- $x_i[SR^{-1}[col : j]]$: The four cells in column j after the SR^{-1} operation is applied, e.g., $x_i[SR^{-1}[col : 0]] = x_i[0, 7, 10, 13]$.
- $x_i[col : j][k, l]$: The j^{th} and l^{th} cells of column j of x_i, e.g., $x_i[col : 0][0, 1] = x_i[0, 4]$.
- $\Delta x_i, \Delta x_i[j]$: The difference at state x_i and cell $x_i[j]$, respectively.

SKINNY is a family of lightweight block ciphers that support two block lengths of $n = 64$ and $n = 128$ bits. In both versions, the internal state *IS* is represented as 4×4 array of cells such that the cell is a nibble (when the block length $n = 64$) or a byte (when the block length $n = 128$). While the classical block ciphers have two inputs, namely the plaintext and the key, and output the ciphertext, SKINNY is a tweakable block cipher [10,9] that uses an input is called the tweakey instead of the key. Then, the user has the freedom to choose which part of the tweakey to be assigned to the key and which part to be assigned to the tweak. This family of block ciphers of block length n deploys three main tweakeys of lengths $t = n$-bit, $t = 2n$-bit and $t = 3n$-bit. Similar to the state, the tweakey state can be represented as z 4×4 arrays of cells, i.e., we have arrays *TK1* (in case $z = 1$), *TK1* and *TK2* (in case $z = 2$), *TK1*, *TK2*, and *TK3* (in case $z = 3$).

First, The plaintext $m = m_0 \| m_1 \| \cdots \| m_{14} \| m_{15}$ (where $|m_i| = n/16 = s$-bit) is loaded into the internal state *IS* row-wise as depicted in Fig. 1. Then, the tweakey input $tk = tk_0 \| tk_1 \| \cdots \| tk_{16z-1}$ (where $|tk_i|$ is s-bit as in the internal state) is loaded row-wise such that $TK1[i] = tk_i$ for $0 \le i \le 15$ (in case $z = 1$), $TK1[i] = tk_i$, $TK2[i] = tk_{16+i}$ for $0 \le i \le 15$ (in case $z = 2$) or $TK1[i] = tk_i$, $TK2[i] = tk_{16+i}$, $TK3[i] = tk_{32+i}$ for $0 \le i \le 15$ (in case $z = 3$). Finally, the internal state is updated by applying the round function r times, where the number of rounds r depends on the block length and the tweakey size, see Table 2.

Table 2. Number of rounds for SKINNY-n-t, with n-bit state and t-bit tweakey state.

Block size n	Tweakey size t		
	n	$2n$	$3n$
64	32	36	40
128	40	48	56

In each round, SKINNY applies five different operations, namely, SubCells, AddConstants, AddRoundTweakey, ShiftRows and MixColumns, see Fig. 1. This cipher does not apply whitening keys. Consequently, parts of the first and last rounds do not add any security. In what follows, we describe the five different operations that are employed in each round:

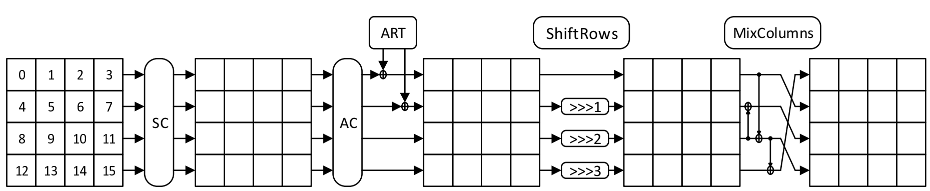

Fig. 1. The SKINNY round function

- SubCells (SC): A nonlinear bijective mapping applied on every cell of the internal state, where 4-bit (in case of $n = 64$) or 8-bit (in case of $n = 128$) S-box is applied. Both S-boxes mapping can be found in [4].
- AddConstants (AC): A 4×4 round constant is XORed to the state. These round constants are generated using a 6-bit affine LFSR. The details of generating the round constants can be found in [4].

– AddRoundTweakey (ART): The first and second rows of all the tweakey arrays are XORed to the state. More precisely, for $0 \leq i \leq 7$, we have:
  - $IS[i] = IS[i] \oplus TK1[i]$, when $z = 1$,
  - $IS[i] = IS[i] \oplus TK1[i] \oplus TK2[i]$, when $z = 2$,
  - $IS[i] = IS[i] \oplus TK1[i] \oplus TK2_i \oplus TK3[i]$, when $z = 3$.

– ShiftRows (SR): The rows of the state are rotated as in AES but to the right, i.e., the following permutation $P = [0, 1, 2, 3, 7, 4, 5, 6, 10, 11, 8, 9, 13, 14\ , 15, 12]$ is applied.

– MixColumns (MC): Each column in the state is multiplied by a binary matrix M, where

$$M = \begin{pmatrix} 1\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,1\,0 \\ 1\,0\,1\,0 \end{pmatrix}$$

Tweakey Schedule. The tweakey arrays are updated through tweakey schedule, see Fig. 2, as follows. First all the tweakey arrays; i.e., $TK1$ (when $z = 1$), $TK1$, $TK2$ (when $z = 2$), or $TK1$, $TK2$, $TK3$ (when $z = 3$); are permuted using a permutation P_T such that $P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$. Finally, each cell in the first and second rows of $TK2$, $TK3$ (when $z = 2$ or $z = 3$) is updated using LFSR, see Table 3, where x_0 is the LSB of the cell.

Table 3. The SKINNY LFSR used in the tweakey schedule

TK	s	LFSR
$TK2$	4	$(x_3 \parallel x_2 \parallel x_1 \parallel x_0) \to (x_2 \parallel x_1 \parallel x_0 \parallel x_3 \oplus x_2)$
	8	$(x_7 \parallel x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 \parallel x_0) \to (x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 \parallel x_0 \parallel x_7 \oplus x_5)$
$TK3$	4	$(x_3 \parallel x_2 \parallel x_1 \parallel x_0) \to (x_0 \oplus x_3 \parallel x_3 \parallel x_2 \parallel x_1)$
	8	$(x_7 \parallel x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1 \parallel x_0) \to (x_0 \oplus x_6 \parallel x_7 \parallel x_6 \parallel x_5 \parallel x_4 \parallel x_3 \parallel x_2 \parallel x_1)$

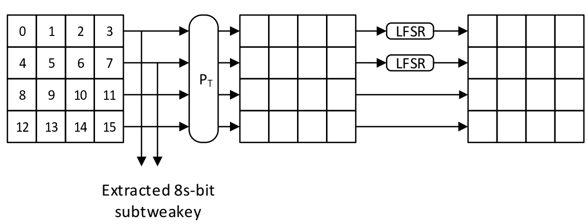

Fig. 2. The tweakey schedule

In our attack, we use AddKey (AK) operation which compromises the AC and ART operations. Moreover, we swap between the linear operations AK, $MC \circ SR$; and hence we use the equivalant subtweakey ETK instead of the subtweakey TK such that $ETK_{r+1} = MC \circ SR(TK_r)$.

3 An Impossible Differential Distinguisher of SKINNY

The impossible differential cryptanalysis was proposed by Biham, Biryukov and Shamir [6]. This attack exploits a (truncated) differential characteristic of probability exactly 0 and thus acts as a distinguisher. Then, this distinguisher can be extended by prepending and/or appending additional rounds, which are usually referred to as the analysis rounds. Finally, the keys that are involved in the analysis round and lead to the impossible differential are excluded. Miss in the Middle is the general technique to construct the impossible differential, where in the cipher $E = E_2 \circ E_1$, we try to find two differentials with probability one, the first one covers the subcipher E_1 and has the form $\Delta\delta \rightarrow \Delta\gamma$; and the second one covers the subcipher E_2^{-1}, and has the form $\Delta\beta \rightarrow \Delta\zeta$, and the intermediate differences $\Delta\gamma, \Delta\zeta$ do not match. Finally, we have the differential $\Delta\delta \rightarrow \Delta\beta$ that covers the whole cipher E and holds with zero probability.

The designers of SKINNY exhaustively searched for the longest truncated impossible differential that has one active cell in the input $\Delta\delta$ and output $\Delta\beta$ of the distinguisher. They found 16 truncated impossible differentials that each one covers 11 rounds of SKINNY. Moreover, they exploited one of these 16 impossible differential distinguishers to attack 16 rounds of SKINNY-n-t ($n = 64$ or $n = 128$).

In our attack, we exploit the same impossible differential distinguisher that was used by the designers to launch impossible differential attacks against SKINNY-n-t ($n = 64$ or $n = 128$). This impossible differential is illustrated in Fig. 3. This distinguisher states that given a pair of message that have only one active cell at $x_3[12]$ cannot have only one active cell at $x_{14}[8]$. The reason is that, the active cell $\Delta x_3[12]$ after 6 rounds will result in 4 active cells and 12 unknown cells at state x_9. From the other side, the active cell $\Delta x_{14}[8]$ will result in 4 inactive cells, 5 unknown cells and 7 active cells at state Y_9. Since the cell at $\Delta x_9[15]$ is active, therefore after the SC operation it should be active (because the S-boxes that are used in all the SKINNY versions are bijective); and this is not the case because $\Delta y_9[15]$ is inactive.

Our attacks depend on the following proposition:

Proposition 1. *(Differential Property of S-box) Given two nonzero differences Δi and Δo in $\mathbb{F}16$ or $\mathbb{F}256$, the equation: $S(x) + S(x + \Delta i) = \Delta o$ has one solution on average. This property also applies to S^{-1}.*

Since all our attacks are based on the same distinguisher, all of these attacks are prepended by 3 rounds and the only structural difference in the appended rounds, we will describe our attack against SKINNY-64-128 in details; then, we will mention the differences in the other attacks.

4 Impossible Differential Key-recovery Attack on 20-round SKINNY-n-$2t$ ($n = 64$ or $n = 128$)

4.1 Impossible Differential Key-recovery Attack of SKINNY-64-128

In this section, we present the first 20-round attack on SKINNY-64-128, as depicted in Fig. 4. The impossible differential attack operates in the chosen plaintext model in order to satisfy the plaintext differences which are obtained from the impossible differential distinguisher. In our attack, we use the idea of structure to generate enough pairs of messages to launch the attack with less amount of required chosen plaintext. In the first three rounds we use the equivalent tweakey ETK instead of the tweakey TK. Therefore, the first round has no tweakey; and hence we can build our structure at $y_1^{'}$. Then, propagate it linearly backward through $MC^{-1}, SR^{-1}, SC^{-1}$ to obtain the corresponding plaintext. Our utilized structure takes all the possible values in 7 nibbles $y_1^{'}[3, 4, 5, 6, 9, 11, 14]$ while the remaining nibbles take a fixed value. Therefore, one structure generates $2^{4\times7} \times (2^{4\times7} - 1)/2 \approx 2^{55}$ possible pairs. Hence, we have 2^{55} possible pairs of messages satisfying the plaintext differences. Moreover, we utilized the following precomputation tables in order to extract the tweakey nibbles involved in the analysis rounds efficiently:

H^*: For any round i, for any column j of the state, and for all the 2^{32} possible values of $\Delta z_i[SR^{-1}[col : j]], z_i[SR^{-1}[col : j]]$, compute $\Delta y_{i+1}[col : j], y_{i+1}[col : j]$. Then, store $\Delta z_i[SR^{-1}[col : j]], z_i[SR^{-1}[col : j]], y_{i+1}[col : j][0, 1]$ in H^* indexed by $\Delta y_{i+1}[col : j], y_{i+1}[col : j][2, 3]$. H^* has 2^{24} rows and on average about $2^{32}/2^{24} = 2^8$ values for each row[1].

[1] We compute this table only once. Then, we use it many times in different rounds and columns.

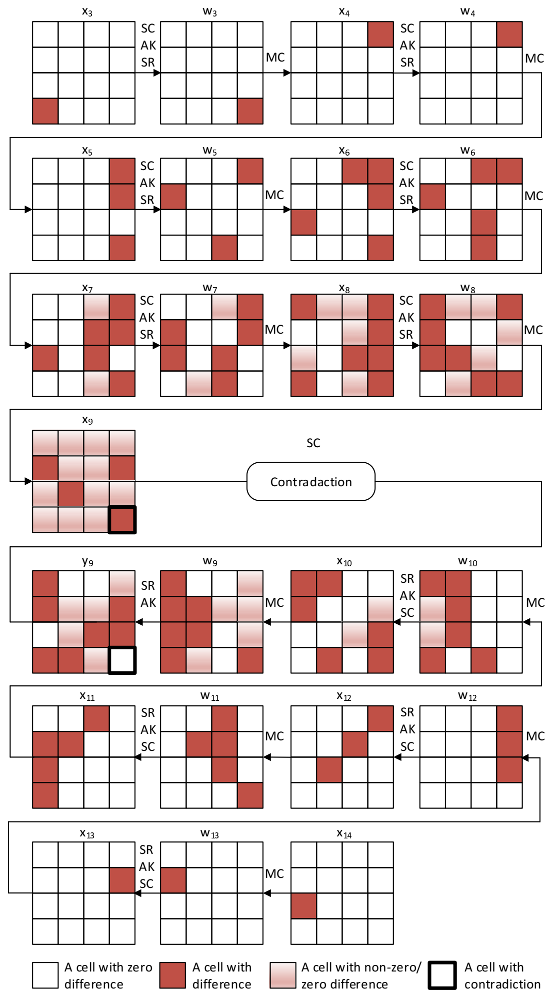

Fig. 3. Impossible differential distinguisher of SKINNY

H_1: For all the 2^{24} possible values of $\Delta z_{17}[SR^{-1}[col:2][0,1]], z_{17}[SR^{-1}[col:2]]$, compute $\Delta y_{18}[col:2], y_{18}[col:2]$. Then, store $\Delta z_{17}[SR^{-1}[col:2][0,1]]$, $z_{17}[SR^{-1}[col:2]], y_{18}[col:2][0,1]$ in H_1 indexed by $\Delta y_{18}[col:2], y_{18}[col:2][2,3]$. H_1 has 2^{24} rows and on average about $2^{24}/2^{24}=1$ value for each row.

H_2: For all the 2^{28} possible values of $\Delta z_{17}[SR^{-1}[col:0][0,2,3]], z_{17}[SR^{-1}[col:0]]$, compute $\Delta y_{18}[col:0], y_{18}[col:0]$. Then, store $\Delta z_{17}[SR^{-1}[col:0][0,2,3]]$, $z_{17}[SR^{-1}[col:0]], y_{18}[col:0][0,1]$ in H_2 indexed by $\Delta y_{18}[col:0], y_{18}[col:0][2,3]$. H_2 has 2^{24} rows and on average about $2^{28}/2^{24}=2^4$ values for each row.

H_3: For all the 2^{28} possible values of $\Delta z_{17}[SR^{-1}[col:3][0,1,3]], z_{17}[SR^{-1}[col:3]]$, compute $\Delta y_{18}[col:3], y_{18}[col:3]$. Then, store $\Delta z_{17}[SR^{-1}[col:3][0,1,3]]$, $z_{17}[SR^{-1}[col:3]], y_{18}[col:3][0,1]$ in H_3 indexed by $\Delta y_{18}[col:3], y_{18}[col:3][2,3]$. H_3 has 2^{24} rows and on average about $2^{28}/2^{24}=2^4$ values for each row.

H_4: For all the 2^{20} possible values of $\Delta z_{16}[SR^{-1}[col:0][0]], z_{16}[SR^{-1}[col:0]]$, compute $\Delta y_{17}[col:0][0,1,3]$, $y_{17}[col:0]$. Then, store $\Delta z_{16}[SR^{-1}[col:0][0]]$, $z_{16}[SR^{-1}[col:0]], y_{17}[col:0][0,1]$ in H_4 indexed by $\Delta y_{17}[col:0][0,1,3], y_{17}[col:0][2,3]$. H_4 has 2^{20} rows and on average about $2^{20}/2^{20}=1$ value for each row.

H_5: From the properties of the MixColumn, we have $\Delta x_{16}[0]=\Delta x_{16}[8]=\Delta x_{16}[12]=\Delta w_{15}[8]$. Therefore, for all the 2^{40} possible values for $\Delta x_{16}[8], x_{16}[8,12], \Delta w_{16}[2,7], w_{16}[2,6,14], x_{17}[3,11]$, compute $w_{16}[10,15]$,

$\Delta y_{17}[2,3,6,10,\ 11,\ 14], y_{17}[2,3,6,10,11,14,15]$ such that $y_{17}[15] = SC([w_{16}[15] \oplus x_{17}[3])$, from the MixColumns operation. Then, store $\Delta z_{16}[SR^{-1}[col:2][0,2]]$, $\Delta z_{16}[SR^{-1}[col:3][1,3]]$, $z_{16}[SR^{-1}[col:2]]$, $z_{16}[SR^{-1}\ [col:3][3]]$, $y_{17}[2,3,6]$ in H_5 indexed by $\Delta y_{17}[2,3,6,10,\ 11,14], y_{17}[10,11,14,15]$. H_5 has 2^{40} rows and on average about $2^{40}/2^{40} = 1$ value for each row.

H_6: For all the 2^{24} possible values of $\Delta z_{16}[SR^{-1}[col:1][0,3]], z_{16}[SR^{-1}[col:1]]$, compute $\Delta y_{17}[col:1][0,1,3], y_{17}[col:1]$. Then, store $\Delta z_{16}[SR^{-1}[col:1][0,3]]$, $z_{16}[SR^{-1}[col:1]], y_{17}[col:1][0,1]$ in H_6 indexed by $\Delta y_{17}[col:1][0,1,3], y_{17}[col:1][2,3]$. H_6 has 2^{20} rows and on average about $2^{24}/2^{20} = 2^4$ values for each row.

H_7: For all the 2^{20} possible values of $\Delta z_{15}[SR^{-1}[col:0][2]], z_{15}[SR^{-1}[col:0]]$, compute $\Delta y_{16}[col:0][0,2,3]$, $y_{16}[col:0]$. Then, store $\Delta z_{15}[SR^{-1}[col:0][2]]$, $z_{15}[SR^{-1}[col:0]], y_{16}[col:0][0]$ in H_7 indexed by $\Delta y_{16}[col:0][0,2,3], y_{16}[col:0][2,3]$. H_7 has 2^{20} rows and on average about $2^{20}/2^{20} = 1$ value for each row.

H_8: For all the 2^{20} possible values of $\Delta z_{15}[SR^{-1}[col:2][0]], z_{15}[SR^{-1}[col:2]]$, compute $\Delta y_{16}[col:2][0,1,3]$, $y_{16}[col:2]$. Then, store $\Delta z_{15}[SR^{-1}[col:2][0]]$, $z_{15}[SR^{-1}[col:2]], y_{16}[col:2][0,1]$ in H_8 indexed by $\Delta y_{16}[col:2][0,1,3], y_{16}[col:2][2,3]$. H_8 has 2^{20} rows and on average about $2^{20}/2^{20} = 1$ value for each row.

H_9: From the properties of the MixColumn, we have $\Delta x_{15}[2] = \Delta x_{15}[10] = \Delta x_{15}[14] = \Delta w_{14}[10]$. Therefore, for all the 2^4 possible differences for $\Delta x_{15}[2,10]$, 2^8 possible values of $x_{15}[2,10]$ and 2^4 possible values of $TK_{15}[2]$, compute $\Delta z_{15}[2\ ,10], z_{15}[2,10]$. Then, store $\Delta z_{15}[2]$ in H_9 indexed by $\Delta z_{15}[2,10], z_{15}[2,10]$,$TK_{15}[2]$. H_9 has 2^{20} rows and on average about $2^{16}/2^{20} = 2^{-4}$ values for each row.

H_{10}: For all the 2^{12} possible differences of $\Delta w_1[5,9,13]$, we have only 2^4 valid differences that have exactly one difference in $\Delta y_2^{'}[13]$ and 3 zero differences in $\Delta y_2^{'}[1,5,9]$. Therefore, for all the 2^4 possible differences of $\Delta w_1[5,9,13]$, 2^{12} possible values of $w_1[5,9,13]$ and 2^8 possible values of $ETK_1[4,14]$, compute $\Delta y_1^{'}[4,14], y_1^{'}[4,14], \Delta x_1[11], x_1[11]$. Then, store $\Delta w_1[5,9\ ,13], w_1[5,9,13], x_1[11]$ in H_{10} indexed by $\Delta y_1^{'}[4,14], y_1^{'}[4,14], \Delta x_1[11]$,$ETK_1[4,14]$. H_{10} has 2^{28} rows and on average about $2^{24}/2^{28} = 2^{-4}$ values for each row.

H_{11}: For all the 2^{12} possible differences of $\Delta w_1[3,7,11]$, we have only 2^4 valid differences that have exactly one difference in $\Delta y_2^{'}[7]$ and 3 zero differences in $\Delta y_2^{'}[3,11,15]$. Therefore, for all the 2^4 possible differences of $\Delta w_1[3,7,11]$, 2^{12} possible values of $w_1[3,7,11]$ and 2^4 possible values of $ETK_1[6]$, compute $\Delta y_1^{'}[6], y_1^{'}[6], \Delta x_1[3,9], x_1[3,9]$. Then, store $\Delta w_1[3,7,11], w_1[3,7,11], x_1[3,9]$ in H_{11} indexed by $\Delta x_1[3,9], \Delta y_1^{'}[6], y_1^{'}[6]$,$ETK_1[6]$. H_{11} has 2^{20} rows and on average about $2^{20}/2^{20} = 1$ value for each row.

H_{12}: For all the 2^8 possible values of $\Delta x_{16}[1], x_{16}[1]$, compute $\Delta y_{16}[1], y_{16}[1]$.Then, store $y_{16}[1]$ in H_{12} indexed by $\Delta y_{16}[1]$. H_{12} has 2^4 rows and on average about $2^8/2^4 = 2^4$ values for each row.

H_{13}: For all the 2^{16} possible values of $\Delta w_1[6], w_1[1,6], ETK_1[1,5]$ ($ETK_1[1] = ETK_1[5]$, see Appendix A), compute $\Delta y_1^{'}[5], y_1^{'}[1,5]$. Then, store $\Delta w_1[6], w_1[1,6]$ in H_{13} indexed by $\Delta y_1^{'}[5], y_1^{'}[1,5]$,$ETK_1[1]$. H_{13} has 2^{16} rows and on average about $2^{16}/2^{16} = 1$ value for each row.

H_{14}: From the properties of the MixColumn, we have $\Delta w_2[4] = \Delta w_2[8] = \Delta w_2[12] = \Delta y_3^{'}[12]$. Therefore, for all the 2^4 possible differences for $\Delta w_2[4,8,12]$, 2^{12} possible values of $w_2[4,8,12]$ and 2^{12} possible values of $ETK_2[7,10,13]$, compute $\Delta y_2^{'}[7,10,13], y_2^{'}[7,10,13]$. Then, store $\Delta y_2^{'}[10]$ in H_{14} indexed by $\Delta y_2^{'}[7,10\ ,13], y_2^{'}[7,13]$,$ETK_2[7,10,13]$. H_{14} has 2^{32} rows and on average about $2^{28}/2^{32} = 2^{-4}$ value for each row.

Using the above mentioned precomputation tables and the utilized structure, our attack proceeds as follows:

1. We take 2^n structures generated as mentioned above. Therefore, we have 2^{n+55} pairs of messages generated using 2^{n+28} messages. Then, ask the encryption oracle for their corresponding ciphertexts; and then decrypted them partially over MC^{-1}, SR^{-1} to compute z_{19}.

2. Determine the number of possible values for $TK_{19}[0:7]$ that satisfy the last round. This can be achieved by performing the following steps for all the message pairs:
   (a) Access H^* for $i = 18, j = 0$ and compute $TK_{19}[0,4]$ such that $TK_{19}[0,4] = y_{19}[0,4] \oplus z_{19}[0,4]$[2]. Therefore, we have 2^8 possible tweakeys for $TK_{19}[0,4]$.
   (b) Access H^* for $i = 18, j = 1$ and compute $TK_{19}[1,5]$ such that $TK_{19}[1,5] = y_{19}[1,5] \oplus z_{19}[1,5]$. Therefore, we have $2^{8+8=16}$ possible tweakeys for $TK_{19}[0,1,4,5]$.
   (c) Access H^* for $i = 18, j = 2$ and compute $TK_{19}[2,6]$ such that $TK_{19}[2,6] = y_{19}[2,6] \oplus z_{19}[2,6]$. Therefore, we have $2^{16+8=24}$ possible tweakeys for $TK_{19}[0,1,2,4,5,6]$.
   (d) Access H^* for $i = 18, j = 3$ and compute $TK_{19}[3,7]$ such that $TK_{19}[3,7] = y_{19}[3,7] \oplus z_{19}[3,7]$. Therefore, we have $2^{24+8=32}$ possible tweakeys for $TK_{19}[0:7]$.
3. Determine the number of possible values for $TK_{18}[0:7]$ that satisfy the nineteenth round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:
   (a) Access H_1 and compute $TK_{18}[2,6]$ such that $TK_{18}[2,6] = y_{18}[2,6] \oplus z_{18}[2,6]$. Therefore, we have 2^{32} possible tweakeys for $TK_{19}[0:7]$,
   $TK_{18}[2,6]$.
   (b) Access H_2 and compute $TK_{18}[0,4]$ such that $TK_{18}[0,4] = y_{18}[0,4] \oplus z_{18}[0,4]$. Therefore, we have $2^{32+4=36}$ possible tweakeys for $TK_{19}[0:7], TK_{18}[0,2,4,6]$.
   (c) Access H_3 and compute $TK_{18}[3,7]$ such that $TK_{18}[3,7] = y_{18}[3,7] \oplus z_{18}[3,7]$. Therefore, we have $2^{36+4=40}$ possible tweakeys for $TK_{19}[0:7], TK_{18}[0,2,3,4,6,7]$.
   (d) Access H^* for $i = 17, j = 1$ and compute $TK_{18}[1,5]$ such that $TK_{18}[1,5] = y_{18}[1,5] \oplus z_{18}[1,5]$. Therefore, we have $2^{40+8=48}$ possible tweakeys for $TK_{19}[0:7], TK_{18}[0:7]$.
4. Determine the number of possible values for $TK_{17}[0:6]$ that satisfy the eighteenth round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:
   (a) Access H_4 and compute $TK_{17}[0,4]$ such that $TK_{17}[0,4] = y_{17}[0,4] \oplus z_{17}[0,4]$. Therefore, we have 2^{48} possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0,4]$.
   (b) Access H_5 and compute $TK_{17}[2,3,6]$ such that $TK_{17}[2,3,6] = y_{17}[2,3,6] \oplus z_{17}[2,3,6]$. Therefore, we have 2^{48} possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0,2,3,4,6]$.
   (c) Access H_6 and compute $TK_{17}[1,5]$ such that $TK_{17}[1,5] = y_{17}[1,5] \oplus z_{17}[1,5]$. Therefore, we have $2^{48+4=52}$ possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$.
5. Determine the number of possible values for $TK_{16}[0,2]$ that satisfy the seventeenth round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:
   (a) Access H_7 and compute $TK_{16}[0]$ such that $TK_{16}[0] = y_{16}[0] \oplus z_{16}[0]$. Therefore, we have 2^{52} possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0]$.
   (b) Access H_8 and compute $TK_{16}[2]$ such that $TK_{16}[2] = y_{16}[2] \oplus z_{16}[2]$. Therefore, we have 2^{52} possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,2]$[3].
6. Using the knowledge of $TK_{15}[2]$, since we know it from the knowledge of $TK_{19}[6]$, $TK_{17}[4]$ (see Appendix A), determine the number of possible tweakey values that satisfy the sixteenth round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:
   (a) Access H_9; and we will find 2^{-4} possible values in each row, i.e., we have 4-bit filter on the remaining tweakeys. Therefore, we have $2^{52-4=48}$ possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,2]$ $TK_{15}[2]$.
7. Using the knowledge of $ETK_1[4,6,14]$ ($ETK_1[6] = ETK_1[14]$), since we know it from the knowledge of $TK_{18}[2,4]$, $TK_{16}[0,2]$ (see Appendix A), determine the number of possible values for $ETK_1[3,9,11]$ that satisfy the second round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:

---

[2] $TK_{19}[0,4] = y_{19}[0,4] \oplus z_{19}[0,4]$ means that $TK_{19}[0] = y_{19}[0] \oplus z_{19}[0]$, $TK_{19}[4] = y_{19}[4] \oplus z_{19}[4]$

[3] Note that instead of having $TK_{16}[6]$ that lead to the impossible differential distinguisher, we have $x_{16}[6]$ that lead to the same impossible differential distinguisher

(a) Access H_{10} and compute $ETK_1[11]$ such that $ETK_1[11] = y_1^{'}[11] \oplus x_1[11]$; we will find 2^{-4} possible values in each row, i.e., we have 4-bit filter on the remaining tweakeys. Therefore, we have $2^{48-4=44}$ possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,2]$, $TK_{15}[2]$, $ETK_1[4,6,11,14]$.

(b) Access H_{11} and compute $ETK_1[3,9]$ such that $ETK_1[3,9] = y_1^{'}[3,9] \oplus x_1[3,9]$. Therefore, we have 2^{44} possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,2]$, $TK_{15}[2]$, $ETK_1[3,4,6,9,11,14]$.

8. Determine the number of possible values for $TK_{16}[1]$ that satisfy the seventeenth round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:

   (a) Access H_{12} and compute $TK_{16}[1]$ such that $TK_{16} = y_{16}[1] \oplus z_{16}[1]$. Therefore, we have $2^{44+4=48}$ possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,1,2]$, $TK_{15}[2]$, $ETK_1[3,4,6,9,11,14]$.

9. Using the knowledge of $ETK_1[1,5]$ ($ETK_1[1] = ETK_1[5]$), since we know it from the knowledge of $TK_{18}[0]$, $TK_{16}[1]$ (see Appendix A), determine the number of possible tweakey values that satisfy the second round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:

   (a) Access H_{13} and we will find 1 possible value in each row. Therefore, we have 2^{48} possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,1,2]$, $TK_{15}[2]$, $ETK_1[1,3,4,5,6,9,11,14]$,.

10. Using the knowledge of $ETK_2[7,10,13]$, since we know it from the knowledge of $TK_{19}[0,3,7]$, $TK_{17}[1,3,5]$ (see Appendix A), determine the number of possible tweakey values that satisfy the third round. This can be achieved by performing the following steps for all the message pairs and remaining tweakeys that satisfy the path until now:

    (a) Access H_{14} and we will find 2^{-4} possible values in each row. Therefore, we have $2^{48-4=44}$ possible tweakeys for $TK_{19}[0:7]$, $TK_{18}[0:7]$, $TK_{17}[0:6]$, $TK_{16}[0,1,2]$, $TK_{15}[2]$, $ETK_1[1,3,4,5,6,9,11,14]$, $ETK_2[7,10,13]$.

Attack Complexity. As depicted in Fig. 4, we have 38 round tweakey nibbles that are involved in the analysis. Thanks to the key schedule, these 38 nibbles take only 2^{116} possible values, see Appendix A. For each of the 2^{n+55} message pairs, we remove, on average, 2^{44} out of 2^{116} possible values of the tweakey nibbles involved in the analysis rounds. Therefore, the probability that a wrong key is not discarded with one pair is $1-2^{44-116} = 1-2^{-72}$. Hence, after processing all the 2^{n+55} pairs, we have $2^{116}(1-2^{-72})^{2^{n+55}} \approx 2^{116} \times 2^{-1.4 \times 2^{n-17}}$ remaining candidates for 116-bit of the tweakey. In order to determine the optimal value of n that will lead to the best computational complexity, we evaluate the computational complexity of the attack as a function of n, as illustrated in Table 4. Analogous to AES [8], the SKINNY round function can be implemented using 16 table lookups. As seen from Table 4, steps 5(a), 5(b) and 6(a) dominate the time complexity of the attack; and hence in order to optimize the time complexity of the attack we choose $n = 19.69$. Consequently, we have 2^{107} remaining key candidates for the 116-bit of the tweakey. Therefore, the tweakey can recovered by exhaustively search the 2^{107} remaining key candidates with 2^{12} remaining tweakey bits, that are not involved in the attack, using 2 plaintext/ciphertext pairs. Therefore, the total time complexity of the attack is $2 \times 2^{107} \times 2^{12} + 2^{120.15} = 2^{121.08}$ encryptions. The data complexity of the attack can be determined from step 1 in which we generate $2^{n=19.69}$ structures. Hence, the data complexity of the attack is $2^{19.69+28=47.69}$ chosen plaintexts. The memory complexity of the attack is dominated by the memory that is required to store $2^{n+55=74.69}$ pairs to exclude the wrong keys; hence, it is $2^{74.69}$.

4.2 Impossible Differential Key-recovery Attack of SKINNY-128-256

Since the only difference between SKINNY-64-128 and SKINNY-128-256 is the key schedule. More precisely, in the LFSR operation. The previous attack on SKINNY-64-128 can be applied on SKINNY-128-256 while only considering that the cell size $s = 8$. Therefore, one structure can generate 2^{111} pairs with 2^{56} chosen plaintexts; and according to the key schedule the 38 bytes involved in the attack have 2^{232} possible values, see the relations in Appendix B. In this attack, we exclude, on overage, 2^{88} out of 2^{232} possible values of the involved tweakey bytes for every message pair. Hence, the probability that one wrong key is not discarded is $1 - 2^{88-232} = 1 - 2^{-144}$. Therefore, we have $2^{232} \times (1 - 2^{-144})^{2^{n+111}} \approx 2^{232} \times 2^{-1.4 \times 2^{n-33}}$ remaining candidates for 232-bit of the tweakey bytes, after processing all the message pairs. In order to optimize the time complexity of the attack, we choose $n = 36.1$. As a result, we have 2^{220} remaining candidates for 232-bit of the tweakey; and hence the tweakey can be recovered by exhaustively searching

Table 4. Time complexity of the different steps of the attack on 20-round SKINNY-64-128, where NT: Number of Tweakeys to be excluded and E: Encryption.

Step	Time Complexity	NT	$n = 19.69$
1	$2^{n+28}E$	-	$2^{47.69}$
2(a)	$2^{n+55} \times \frac{1}{16 \times 20} \approx 2^{n+46.68}E$	2^8	$2^{66.37}$
2(b)	$2^{n+55} \times 2^8 \times \frac{1}{16 \times 20} \approx 2^{n+54.68}E$	2^{16}	$2^{74.37}$
2(c)	$2^{n+55} \times 2^{16} \times \frac{1}{16 \times 20} \approx 2^{n+62.68}E$	2^{24}	$2^{82.37}$
2(d)	$2^{n+55} \times 2^{24} \times \frac{1}{16 \times 20} \approx 2^{n+70.68}E$	2^{32}	$2^{90.37}$
3(a)	$2^{n+55} \times 2^{32} \times \frac{1}{16 \times 20} \approx 2^{n+78.68}E$	2^{32}	$2^{98.37}$
3(b)	$2^{n+55} \times 2^{32} \times \frac{1}{16 \times 20} \approx 2^{n+78.68}E$	2^{36}	$2^{98.37}$
3(c)	$2^{n+55} \times 2^{36} \times \frac{1}{16 \times 20} \approx 2^{n+82.68}E$	2^{40}	$2^{102.37}$
3(d)	$2^{n+55} \times 2^{40} \times \frac{1}{16 \times 20} \approx 2^{n+86.68}E$	2^{48}	$2^{106.37}$
4(a)	$2^{n+55} \times 2^{48} \times \frac{1}{16 \times 20} \approx 2^{n+94.68}E$	2^{48}	$2^{114.37}$
4(b)	$2^{n+55} \times 2^{48} \times \frac{2}{16 \times 20} \approx 2^{n+95.68}E$	2^{48}	$2^{115.37}$
4(c)	$2^{n+55} \times 2^{48} \times \frac{1}{16 \times 20} \approx 2^{n+94.68}E$	2^{52}	$2^{114.37}$
5(a)	$2^{n+55} \times 2^{52} \times \frac{1}{16 \times 20} \approx 2^{n+98.68}E$	2^{52}	$2^{118.37}$
5(b)	$2^{n+55} \times 2^{52} \times \frac{1}{16 \times 20} \approx 2^{n+98.68}E$	2^{52}	$2^{118.37}$
6(a)	$2^{n+55} \times 2^{52} \times \frac{1}{16 \times 20} \approx 2^{n+98.68}E$	2^{48}	$2^{118.37}$
7(a)	$2^{n+55} \times 2^{48} \times \frac{1}{16 \times 20} \approx 2^{n+94.68}E$	2^{44}	$2^{114.37}$
7(b)	$2^{n+55} \times 2^{44} \times \frac{1}{16 \times 20} \approx 2^{n+90.68}E$	2^{44}	$2^{110.37}$
8(a)	$2^{n+55} \times 2^{44} \times \frac{1}{16 \times 20} \approx 2^{n+90.68}E$	2^{48}	$2^{110.37}$
9(a)	$2^{n+55} \times 2^{48} \times \frac{1}{16 \times 20} \approx 2^{n+94.68}E$	2^{48}	$2^{114.37}$
10(a)	$2^{n+55} \times 2^{48} \times \frac{1}{16 \times 20} \approx 2^{n+94.68}E$	2^{44}	$2^{114.37}$

the remaining candidates with 2^{24} possible values, for the 24-bit of the tweakey that are not involved in the attack, using 2 plaintext/ciphertext pairs. Therefore, the total time complexity of the attack is $2 \times 2^{220} \times 2^{24} + 2^{36.1+111} \times 2^{104} \times \frac{3}{16 \times 20}$[4]$= 2^{245} + 2^{244.36} = 2^{245.72}$. The data complexity of the attack is $2^{n+56=92.1}$ chosen plaintexts; and the memory complexity is dominated by storing $2^{n+111=147.1}$ message pairs.

5 Impossible Differential Key-recovery Attack on 18-round SKINNY-n-n ($n = 64$ or $n = 128$)

The only difference between SKINNY-64-64 and SKINNY-128-128 is the cell size s, where $s = 4$ (resp. $s = 8$) in case of SKINNY-64-64 (resp. SKINNY-128-128). Therefore, we present the steps of the two attacks concurrently as a function of s. This attack is applicable to the first 18 rounds of the previous attack, i.e., the ciphertext $c = x_{18}$. Therefore, we use the same steps used in the previous attack from step 4 to the end and the same precomputation tables from H_4 to the end with the following modifications:

- Step 1, each structure can generate $2^{7\times s} \times 2^{7\times s-1} = 2^{14\times s-1}$ with $2^{7\times s}$ chosen plaintexts. Then, to apply the attack we take 2^n structures to generate $2^{n+14\times s-1}$ pairs, but we have 4 s-bit filter in the transition over MC^{-1} from the ciphertext to w_{17}. Therefore, we have $2^{n+14\times s-1-4\times s=n+10\times s-1}$ remaining pairs to launch the attack.
- The number of rows and entries in each table will be represented as a function of s. For example, H_6 has $2^{5\times s}$ rows; and in each row, we have 2^s entries.
- The modifications of the number of Tweakeys to be excluded from step 4 to the end are presented in Table 5.
- For the relation of the tweakey cells, see Appendix C.

Attack Complexity. We have 22 tweakey cells that are involved in the analysis rounds; these 22 tweakey cells have only $2^{13\times s}$ possible values, refer to Appendix C. The probability that one wrong key is not discarded with one pair is $1 - 2^{-s-13\times s} = 1 - 2^{-14\times s}$. Hence, after processing all the $2^{n+10\times s-1}$ pairs, we have $2^{13\times s}(1-2^{-14\times s})^{2^{n+10\times s-1}} \approx 2^{13\times s} \times 2^{-1.4\times 2^{n-4\times s-1}}$ remaining candidates for $13\times s$-bit of the tweakey. Steps 5(a), 5(b) and 6(a) dominate the time complexity of the attack, as seen from Table 5; and hence in order to optimize the time complexity of the attack we choose $n = 19.52$ (resp. $n = 36.42$) in case of SKINNY-64-64 (resp. SKINNY-128-128). Consequently, we have 2^{44} (resp. 2^{89}) remaining key candidates for the 52-bit (resp. 104-bit) of the tweakey. Therefore, the tweakey can be recovered by exhaustively searching the 2^{44} (resp. 2^{89}) remaining key candidates with 2^{12} (resp. 2^{24}) for the other tweakey bits, that are not involved in the attack, using 1 plaintext/ciphertext pair. Therefore, the total time complexity of the attack is $2^{44} \times 2^{12} + 2^{56.14} = 2^{57.1}$ (resp. $2^{89} \times 2^{24} + 2^{116.84} = 2^{116.94}$) encryptions in case of SKINNY-64-64 (resp. SKINNY-128-128). The data complexity of the attack can be determined from step 1 in which we generate $2^{n=19.52}$ (resp. $2^{n=36.42}$) structures. Hence, the data complexity of the attack is $2^{19.52+28=47.52}$ (resp. $2^{36.42+56=92.42}$) chosen plaintexts in case of SKINNY-64-64 (resp. SKINNY-128-128). The memory complexity of the attack is $2^{58.52}$ (resp. $2^{115.42}$) that are required to store the $2^{58.52}$ (resp. $2^{115.42}$) pairs after the ciphertext filtration to exclude the wrong keys in case of SKINNY-64-64 (resp. SKINNY-128-128).

6 Impossible Differential Key-recovery Attack on 22-round SKINNY-n-$3n$ ($n = 64$ or $n = 128$)

SKINNY-64-192 differs from SKINNY-128-384 in the cell size s and the tweakey schedule. As the tweakey schedule does not influence the attack procedure, we present the two attacks as a function of s. The previous 20-round attack of SKINNY-n-$2n$ ($n = 64$ or $n = 128$) can be extended to 22-round attack on SKINNY-n-$3n$ ($n = 64$ or $n = 128$) by appending 2 rounds, i.e., the ciphertext $c = x_{22}$. Therefore, we can use the same attack procedures of SKINNY-n-$2n$ ($n = 64$ or $n = 128$) to attack SKINNY-n-$3n$ ($n = 64$ or $n = 128$) by repeating step 2 three times to extract the tweakey cells $TK_{19}[0:7]$, $TK_{20}[0:7]$, $TK_{21}[0:7]$,

[4] The second term is computed from step 5(a),5(b) and 6(a).

the details of the tweakey schedule can be found in Appendix D. Moreover, as in the previous attack on 18-round SKINNY-n-n ($n = 64$ or $n = 128$), each structure can generate $2^{7\times s} \times 2^{7\times s-1} = 2^{14\times s-1}$ with $2^{7\times s}$ chosen plaintexts. Then, we take 2^n structures to generate $2^{n+14\times s-1}$ pairs using $2^{n+7\times s}$ chosen plaintexts.

Attack Complexity. We have 54 tweakey cells that are involved in the analysis rounds; these 54 tweakey cells have only $2^{45\times s}$ possible values. The probability that one wrong key is not discarded with one pair is $1 - 2^{27\times s-45\times s} = 1 - 2^{-18\times s}$. Hence, after processing all the $2^{n+14\times s-1}$ pairs, we have $2^{45\times s}(1 - 2^{-18\times s})^{2^{n+14\times s-1}} \approx 2^{45\times s} \times 2^{-1.4\times 2^{n-4\times s-1}}$ remaining candidates for $45 \times s$-bit of the tweakey. In order to optimize the time complexity of the attack we choose $n = 19.84$ (resp. $n = 36.22$) in case of SKINNY-64-192 (resp. SKINNY-128-384). Consequently, we have 2^{170} (resp. 2^{347}) remaining key candidates for the 180-bit (resp. 360-bit) of the tweakey. Therefore, the tweakey can be recovered by exhaustively searching the 2^{170} (resp. 2^{347}) remaining key candidates with 2^{12} (resp. 2^{24}) for the other tweakey bits, that are not involved in the attack, using 3 plaintext/ciphertext pairs. Therefore, the total time complexity of the attack is $3 \times 2^{170} \times 2^{12} + 2^{183.97} = 2^{184.79}$ (resp. $3 \times 2^{347} \times 2^{24} + 2^{372.35} = 2^{373.48}$) encryptions in case of SKINNY-64-192 (resp. SKINNY-128-384). The data complexity of the attack is $2^{19.84+28=47.84}$ (resp. $2^{36.22+56=92.22}$) chosen plaintexts in case of SKINNY-64-192 (resp. SKINNY-128-384). The memory complexity of the attack is $2^{74.84}$ (resp. $2^{147.22}$) in case of SKINNY-64-64 (resp. SKINNY-128-384).

Table 5. Time complexity of the different steps of the attack on 18-round SKINNY-64-64 and SKINNY-128-128, where NT: Number of Tweakeys to be excluded and E: Encryption.

Step	Time Complexity	NT	$s = 4, n = 19.52$	$s = 8, n = 36.42$
1	$2^{n+7\times s}E$	-	$2^{47.52}$	$2^{92.42}$
4(a)	$2^{n+10\times s-1} \times \frac{1}{16\times 18} \approx 2^{n+10\times s-9.17}E$	1	$2^{50.35}$	$2^{107.25}$
4(b)	$2^{n+10\times s-1} \times \frac{2}{16\times 18} \approx 2^{n+10\times s-8.17}E$	1	$2^{51.35}$	$2^{108.25}$
4(c)	$2^{n+10\times s-1} \times \frac{1}{16\times 18} \approx 2^{n+10\times s-9.17}E$	2^s	$2^{50.35}$	$2^{107.25}$
5(a)	$2^{n+10\times s-1} \times 2^s \times \frac{1}{16\times 18} \approx 2^{n+11\times s-9.17}E$	2^s	$2^{54.35}$	$2^{115.25}$
5(b)	$2^{n+10\times s-1} \times 2^s \times \frac{1}{16\times 18} \approx 2^{n+11\times s-9.17}E$	2^s	$2^{54.35}$	$2^{115.25}$
6(a)	$2^{n+10\times s-1} \times 2^s \times \frac{1}{16\times 18} \approx 2^{n+11\times s-9.17}E$	1	$2^{54.35}$	$2^{115.25}$
7(a)	$2^{n+10\times s-1} \times \frac{1}{16\times 18} \approx 2^{n+10\times s-9.17}E$	2^{-s}	$2^{50.35}$	$2^{107.25}$
7(b)	$2^{n+10\times s-1} \times 2^{-s} \times \frac{1}{16\times 18} \approx 2^{n+9\times s-9.17}E$	2^{-s}	$2^{46.35}$	$2^{99.25}$
8(a)	$2^{n+10\times s-1} \times 2^{-s} \times \frac{1}{16\times 18} \approx 2^{n+9\times s-9.17}E$	1	$2^{46.35}$	$2^{99.25}$
9(a)	$2^{n+10\times s-1} \times \frac{1}{16\times 18} \approx 2^{n+10\times s-9.17}E$	1	$2^{50.35}$	$2^{107.25}$
10(a)	$2^{n+10\times s-1} \times \frac{1}{16\times 18} \approx 2^{n+10\times s-9.17}E$	2^{-s} [5]	$2^{50.35}$	$2^{107.25}$

[5] After this step, we have 2^{-s} tweakeys to be excluded for each message pair, i.e., we exclude 1 tweakey after processing 2^s pairs.

7 Conclusion

In this work, we presented impossible differential attacks against all the 6 variants of SKINNY. All of these attacks use the same impossible differential distinguisher that covers 11-round. We extended these 11-round by 7, 9 and 11 rounds to attack 18, 20 and 22 rounds of SKINNY-n-n, SKINNY-n-$2n$ and SKINNY-n-$3n$ ($n = 64$ or $n = 128$), respectively, exploiting that the tweakey is only added to the first two rows with the MixColumns operation properties and the simple tweakey schedule.

References

1. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L. The simon and speck families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.
2. Beierle, C., Jean, J., Klbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., and Sim, S. M. The skinny family of block ciphers and its low-latency variant mantis. Cryptology ePrint Archive, Report 2016/660, 2016. http://eprint.iacr.org/2016/660.
3. Beierle, C., Jean, J., Klbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., and Sim, S. M. Skinny family of block ciphers: Cryptanalysis competition, 2016.
4. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., and Sim, S. M. The skinny family of block ciphers and its low-latency variant mantis. In *Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, M. Robshaw and J. Katz, Eds. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016, pp. 123–153.
5. Benadjila, R., Guo, J., Lomné, V., and Peyrin, T. Implementing lightweight block ciphers on x86 architectures. In *Selected Areas in Cryptography – SAC 2013: 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, T. Lange, K. Lauter, and P. Lisoněk, Eds. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 324–351.
6. Biham, E., Biryukov, A., and Shamir, A. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In *Advances in Cryptology - EUROCRYPT 99*, J. Stern, Ed., vol. 1592 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 1999, pp. 12–23.
7. Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., and Rijmen, V. A more efficient aes threshold implementation. In *Progress in Cryptology – AFRICACRYPT 2014: 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, D. Pointcheval and D. Vergnaud, Eds. Springer International Publishing, Cham, 2014, pp. 267–284.
8. Daemen, J., and Rijmen, V. *The Design of Rijndael*. Springer-Verlag New York, Inc., 2002.
9. Jean, J., Nikolić, I., and Peyrin, T. Tweaks and keys for block ciphers: The tweakey framework. In *Advances in Cryptology – ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, P. Sarkar and T. Iwata, Eds. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 274–288.
10. Liskov, M., Rivest, R. L., and Wagner, D. Tweakable block ciphers. *Journal of Cryptology 24*, 3 (2011), 588–613.
11. Peyrin, T., and Seurin, Y. Counter-in-tweak: Authenticated encryption modes for tweakable block ciphers. In *Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, M. Robshaw and J. Katz, Eds. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016, pp. 33–63.

A SKINNY-64-128 Key schedule relations

Tables 6, 7 illustrate the tweakey and equivalent tweakey relations, respectively, that are considered in the analysis rounds. We have 28 tweakey nibbles and 10 equivalent tweakey nibbles that are used in the analysis rounds. In this section, we show that these tweakey and equivalent tweakey nibbles have only 2^{116} possible values, thanks to the key schedule.

For the tweakey nibbles $TK_{17}[t], t = \{0, 1, 2, 3, 4, 5, 6\}$ and $TK_{19}[f], f = \{2, 0, 4\ , 7, 6, 3, 5\}$, the following relations hold:

$$\begin{aligned} TK_{17}[t][0] &= TK1[l][0] \oplus TK2[l]\{0, 1, 2, 3\} & TK_{19}[f][0] &= TK1[l][0] \oplus TK2[l]\{0, 1, 3\} \\ TK_{17}[t][1] &= TK1[l][1] \oplus TK2[l]\{0, 1, 2\} & TK_{19}[f][1] &= TK1[l][1] \oplus TK2[l]\{0, 1, 2, 3\} \\ TK_{17}[t][2] &= TK1[l][2] \oplus TK2[l]\{1, 2, 3\} & TK_{19}[f][2] &= TK1[l][2] \oplus TK2[l]\{0, 1, 2\} \\ TK_{17}[t][3] &= TK1[l][3] \oplus TK2[l]\{0, 2\} & TK_{19}[f][3] &= TK1[l][3] \oplus TK2[l]\{1, 2, 3\}, \end{aligned}$$

where $l = 9, 15, 8, 13, 10, 14, 12$. From the above relations we can deduce $TK1[l]$, $TK2[l]$. Therefore, we have $2^{2\times7\times4=56}$ possible values for these 14 nibbles. Moreover, the knowledge of $TK1[e], TK2[e]$, where $e = 13, 14, 15$ allows us to deduce the values of $ETK_2[7, 10, 13]$; and the knowledge of of $TK1[10]$, $TK2[10]$ allows us to deduce the value of $TK_{15}[2]$. In addition, we have 2^4 possible values for the nibble $TK_{19}[1]$. Therefore, we have $2^{56+4=60}$ possible values for the 19 tweakey nibbles that are involved in rounds 3, 16, 18, 20.

For the tweakey nibbles $TK_{16}[t], t = \{0, 1, 2\}$ and $TK_{18}[f]\ , f = \{2, 0, 4\}$, the following relations hold:

$$\begin{aligned} TK_{16}[t][0] &= TK1[l][0] \oplus TK2[l]\{0, 1, 2\} & TK_{18}[f][0] &= TK1[l][0] \oplus TK2[l]\{0, 1, 2, 3\} \\ TK_{16}[t][1] &= TK1[l][1] \oplus TK2[l]\{1, 2, 3\} & TK_{18}[f][1] &= TK1[l][1] \oplus TK2[l]\{0, 1, 2\} \\ TK_{16}[t][2] &= TK1[l][2] \oplus TK2[l]\{0, 2\} & TK_{18}[f][2] &= TK1[l][2] \oplus TK2[l]\{1, 2, 3\} \\ TK_{16}[t][3] &= TK1[l][3] \oplus TK2[l]\{1, 3\} & TK_{18}[f][3] &= TK1[l][3] \oplus TK2[l]\{0, 2\}, \end{aligned}$$

where $l = 0, 1, 2$. From the above relations we can deduce $TK1[l]$, $TK2[l]$. Therefore, we have $2^{2\times3\times4=24}$ possible values for these 6 nibbles. Moreover, the knowledge of $TK1[l]$, $TK2[l]$ allows us to deduce the values of $ETK_1[1, 4, 5, 6, 14]$. Hence, we have 2^{24} possible values for the 10 tweakey nibbles that are involved in rounds 2, 17, 19.

For the tweakey nibbles $ETK_1[t], t = \{3, 9, 11\}$ and $TK_{18}[f]\ , f = \{7, 6, 5\}$, the following relations hold:

$$\begin{aligned} ETK_1[t][0] &= TK1[l][0] \oplus TK2[l]\{0\} & TK_{18}[f][0] &= TK1[l][0] \oplus TK2[l]\{0, 1, 2, 3\} \\ ETK_1[t][1] &= TK1[l][1] \oplus TK2[l]\{1\} & TK_{18}[f][1] &= TK1[l][1] \oplus TK2[l]\{0, 1, 2\} \\ ETK_1[t][2] &= TK1[l][2] \oplus TK2[l]\{2\} & TK_{18}[f][2] &= TK1[l][2] \oplus TK2[l]\{1, 2, 3\} \\ ETK_1[t][3] &= TK1[l][3] \oplus TK2[l]\{3\} & TK_{18}[f][3] &= TK1[l][3] \oplus TK2[l]\{0, 2\}, \end{aligned}$$

where $l = 3, 4, 6$. From the above relations we can deduce $TK1[l]$, $TK2[l]$. Moreover, the knowledge of $TK1[6]$, $TK2[6]$ allows us to deduce the values of $TK_{16}[6]$ Therefore, we have $2^{2\times3\times4=24}$ possible values for these 7 nibbles. In addition, we have 2^8 possible values of $TK_{18}[1, 3]$. Hence, we have $2^{24+8=32}$ possible values for the 9 tweakey nibbles that are involved in rounds 2, 17, 19.

B SKINNY-128-256 Key schedule relations

Tables 8, 9 illustrate the tweakey and equivalent tweakey relations, respectively.

Table 6. SKINNY-64-128 tweakey relations for round $i = 15, 16, \cdots, 19$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i = 15$, $TK_i[j, j = 0:7] = L_1^8(TK1[l]) \oplus L_2^8(TK2[l])$, $l = 8, 9, 10, 11, 12, 13, 14, 15$ and Round $i = 16$, $TK_i[j, j = 0:7] = L_1^8(TK1[l]) \oplus L_2^8(TK2[l])$, $l = 0, 1, 2, 3, 4, 5, 6, 7$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,1,2\}$	$TK1[l][1] \oplus TK2[l]\{1,2,3\}$	$TK1[l][2] \oplus TK2[l]\{0,2\}$	$TK1[l][3] \oplus TK2[l]\{1,3\}$
Round $i = 17$, $TK_i[j, j = 0:7] = L_1^9(TK1[l]) \oplus L_2^9(TK2[l])$, $l = 9, 15, 8, 13, 10, 14, 12, 11$ and Round $i = 18$, $TK_i[j, j = 0:7] = L_1^9(TK1[l]) \oplus L_2^9(TK2[l])$, $l = 1, 7, 0, 5, 2, 6, 4, 3$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,1,2,3\}$	$TK1[l][1] \oplus TK2[l]\{0,1,2\}$	$TK1[l][2] \oplus TK2[l]\{1,2,3\}$	$TK1[l][3] \oplus TK2[l]\{0,2\}$
Round $i = 19$, $TK_i[j, j = 0:7] = L_1^{10}(TK1[l]) \oplus L_2^{10}(TK2[l])$, $l = 15, 11, 9, 14, 8, 12, 10, 13$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,1,3\}$	$TK1[l][1] \oplus TK2[l]\{0,1,2,3\}$	$TK1[l][2] \oplus TK2[l]\{0,1,2\}$	$TK1[l][3] \oplus TK2[l]\{1,2,3\}$

Table 7. SKINNY-64-128 equivlant tweakey relations for round $i = 1, 2$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i = 1$, $ETK_i[j, j = 0:15] = TK1[l] \oplus TK2[l]$, $l = 0, 1, 2, 3, 0, 1, 2, 3, 7, 4, 5, 6, 0, 1, 2, 3$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l][0]$	$TK1[l][1] \oplus TK2[l][1]$	$TK1[l][2] \oplus TK2[l][2]$	$TK1[l][3] \oplus TK2[l][3]$
Round $i = 2$, $ETK_i[j, j = 0:15] = L_1(TK1[l]) \oplus L_2(TK2[l])$, $l = 9, 15, 8, 13, 9, 15, 8, 13, 11, 10, 14, 12, 9, 15, 8, 13$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{2,3\}$	$TK1[l][1] \oplus TK2[l][0]$	$TK1[l][2] \oplus TK2[l][1]$	$TK1[l][3] \oplus TK2[l][2]$

Table 8. SKINNY-128-256 tweakey relations for round $i = 15, 16, \cdots, 19$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i = 15$, $TK_i[j, j = 0 : 7] = L_1^8(TK1[l]) \oplus L_2^8(TK2[l])$, $l = 8, 9, 10, 11, 12, 13, 14, 15$
and Round $i = 16$, $TK_i[j, j = 0 : 7] = L_1^8(TK1[l]) \oplus L_2^8(TK2[l])$, $l = 0, 1, 2, 3, 4, 5, 6, 7$

$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,4,6\}$	$TK1[l][1] \oplus TK2[l]\{1,5,7\}$	$TK1[l][2] \oplus TK2[l]\{0,2\}$	$TK1[l][3] \oplus TK2[l]\{1,3\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$TK1[l][4] \oplus TK2[l]\{2,4\}$	$TK1[l][5] \oplus TK2[l]\{3,5\}$	$TK1[l][6] \oplus TK2[l]\{4,6\}$	$TK1[l][7] \oplus TK2[l]\{5,7\}$

Round $i = 17$, $TK_i[j, j = 0 : 7] = L_1^9(TK1[l]) \oplus L_2^9(TK2[l])$, $l = 9, 15, 8, 13, 10, 14, 12, 11$
and Round $i = 18$, $TK_i[j, j = 0 : 7] = L_1^9(TK1[l]) \oplus L_2^9(TK2[l])$, $l = 1, 7, 0, 5, 2, 6, 4, 3$

$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{3,7\}$	$TK1[l][1] \oplus TK2[l]\{0,4,6\}$	$TK1[l][2] \oplus TK2[l]\{1,5,7\}$	$TK1[l][3] \oplus TK2[l]\{0,2\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$TK1[l][4] \oplus TK2[l]\{1,3\}$	$TK1[l][5] \oplus TK2[l]\{2,4\}$	$TK1[l][6] \oplus TK2[l]\{3,5\}$	$TK1[l][7] \oplus TK2[l]\{4,6\}$

Round $i = 19$, $TK_i[j, j = 0 : 7] = L_1^{10}(TK1[l]) \oplus L_2^{10}(TK2[l])$, $l = 15, 11, 9, 14, 8, 12, 10, 13$

$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{2,6\}$	$TK1[l][1] \oplus TK2[l]\{3,7\}$	$TK1[l][2] \oplus TK2[l]\{0,4,6\}$	$TK1[l][3] \oplus TK2[l]\{1,5,7\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$TK1[l][4] \oplus TK2[l]\{0,2\}$	$TK1[l][5] \oplus TK2[l]\{1,3\}$	$TK1[l][6] \oplus TK2[l]\{2,4\}$	$TK1[l][7] \oplus TK2[l]\{3,5\}$

Table 9. SKINNY-128-256 equivlant tweakey relations for round $i = 1, 2$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i=1$, $ETK_i[j, j=0:15] = TK1[l] \oplus TK2[l], l = 0,1,2,3,0,1,2,3,7,4,5,6,0,1,2,3$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l][0]$	$TK1[l][1] \oplus TK2[l][1]$	$TK1[l][2] \oplus TK2[l][2]$	$TK1[l][3] \oplus TK2[l][3]$
$ETK_i[j][4]$	$ETK_i[j][5]$	$ETK_i[j][6]$	$ETK_i[j][7]$
$TK1[l][4] \oplus TK2[l][4]$	$TK1[l][5] \oplus TK2[l][5]$	$TK1[l][6] \oplus TK2[l][6]$	$TK1[l][7] \oplus TK2[l][7]$
Round $i=2$, $ETK_i[j, j=0:15] = L_1(TK1[l]) \oplus L_2(TK2[l])$, $l = 9,15,8,13,9,15,8,13,11,10,14,12,9,15,8,13$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{5,7\}$	$TK1[l][1] \oplus TK2[l][0]$	$TK1[l][2] \oplus TK2[l][1]$	$TK1[l][3] \oplus TK2[l][2]$
$ETK_i[j][4]$	$ETK_i[j][5]$	$ETK_i[j][6]$	$ETK_i[j][7]$
$TK1[l][4] \oplus TK2[l][3]$	$TK1[l][5] \oplus TK2[l][4]$	$TK1[l][6] \oplus TK2[l][5]$	$TK1[l][7] \oplus TK2[l][6]$

C SKINNY-64-64 and SKINNY-128-128 Key schedule relations

Tables 10, 11 illustrate the tweakey and equivalent tweakey relations, respectively.

Table 10. SKINNY-64-64 and SKINNY-128-128 tweakey relations for round $i = 15, 16, 17$.

Round $i = 15$	$TK_i[j, j=0:7] = TK1[l]$, $l = 8,9,10,11,12,13,14,15$
Round $i = 16$	$TK_i[j, j=0:7] = TK1[l]$, $l = 0,1,2,3,4,5,6,7$
Round $i = 17$	$TK_i[j, j=0:7] = TK1[l]$, $l = 9,15,8,13,10,14,12,11$

Table 11. SKINNY-64-64 and SKINNY-128-128 equivlant tweakey relations for round $i = 1, 2$.

Round $i = 1$	$ETK_i[j, j=0:15] = TK1[l], l = 0,1,2,3,0,1,2,3,7,4,5,6,0,1,2,3$
Round $i = 2$	$ETK_i[j, j=0:15] = TK1[l], l = 9,15,8,13,9,15,8,13,11,10,14,12,9,15,8,13$

D SKINNY-64-192 and SKINNY-128-384 Key schedule relations

Tables 12, 13 (resp. 14, 15) illustrate the tweakey and equivalent tweakey relations of SKINNY-64-192 (resp. SKINNY-128-384).

Table 12. SKINNY-64-192 tweakey relations for round $i = 15, 16, \cdots, 21$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i = 15$, $TK_i[j, j = 0:7] = L_1^8(TK1[l]) \oplus L_2^8(TK2[l]) \oplus L_2^8(TK3[l])$, $l = 8, 9, 10, 11, 12, 13, 14, 15$ and Round $i = 16$, $TK_i[j, j = 0:7] = L_1^8(TK1[l]) \oplus L_2^8(TK2[l]) \oplus L_2^8(TK3[l])$, $l = 0, 1, 2, 3, 4, 5, 6, 7$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,1,2\}$ $\oplus TK3[l]\{1,2,3\}$	$TK1[l][1] \oplus TK2[l]\{1,2,3\}$ $\oplus TK3[l]\{0,2\}$	$TK1[l][2] \oplus TK2[l]\{0,2\}$ $\oplus TK3[l]\{1,3\}$	$TK1[l][3] \oplus TK2[l]\{1,3\}$ $\oplus TK3[l]\{0,2,3\}$
Round $i = 17$, $TK_i[j, j = 0:7] = L_1^9(TK1[l]) \oplus L_2^9(TK2[l]) \oplus L_2^9(TK3[l])$, $l = 9, 15, 8, 13, 10, 14, 12, 11$ and Round $i = 18$, $TK_i[j, j = 0:7] = L_1^9(TK1[l]) \oplus L_2^9(TK2[l]) \oplus L_2^9(TK3[l])$, $l = 1, 7, 0, 5, 2, 6, 4, 3$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,1,2,3\}$ $\oplus TK3[l]\{0,2\}$	$TK1[l][1] \oplus TK2[l]\{0,1,2\}$ $\oplus TK3[l]\{1,3\}$	$TK1[l][2] \oplus TK2[l]\{1,2,3\}$ $\oplus TK3[l]\{0,2,3\}$	$TK1[l][3] \oplus TK2[l]\{0,2\}$ $\oplus TK3[l]\{0,1\}$
Round $i = 19$, $TK_i[j, j = 0:7] = L_1^{10}(TK1[l]) \oplus L_2^{10}(TK2[l]) \oplus L_2^{10}(TK3[l])$, $l = 15, 11, 9, 14, 8, 12, 10, 13$ and Round $i = 20$, $TK_i[j, j = 0:7] = L_1^{10}(TK1[l]) \oplus L_2^{10}(TK2[l]) \oplus L_2^{10}(TK3[l])$, $l = 7, 3, 1, 6, 0, 4, 2, 5$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,1,3\}$ $\oplus TK3[l]\{1,3\}$	$TK1[l][1] \oplus TK2[l]\{0,1,2,3\}$ $\oplus TK3[l]\{0,2,3\}$	$TK1[l][2] \oplus TK2[l]\{0,1,2\}$ $\oplus TK3[l]\{0,1\}$	$TK1[l][3] \oplus TK2[l]\{1,2,3\}$ $\oplus TK3[l]\{1,2\}$
Round $i = 21$, $TK_i[j, j = 0:7] = L_1^{11}(TK1[l]) \oplus L_2^{11}(TK2[l]) \oplus L_2^{11}(TK3[l])$, $l = 11, 13, 15, 12, 9, 10, 8, 14$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{0,3\}$ $\oplus TK3[l]\{0,2,3\}$	$TK1[l][1] \oplus TK2[l]\{0,1,3\}$ $\oplus TK3[l]\{0,1\}$	$TK1[l][2] \oplus TK2[l]\{0,1,2,3\}$ $\oplus TK3[l]\{1,2\}$	$TK1[l][3] \oplus TK2[l]\{0,1,2\}$ $\oplus TK3[l]\{2,3\}$

Table 13. SKINNY-64-192 equivlant tweakey relations for round $i = 1, 2$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i = 1$, $ETK_i[j, j = 0:15] = TK1[l] \oplus TK2[l] \oplus TK3[l]$,$l = 0, 1, 2, 3, 0, 1, 2, 3$,$7, 4, 5, 6, 0, 1, 2, 3$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l][0]$ $\oplus TK3[l][0]$	$TK1[l][1] \oplus TK2[l][1]$ $\oplus TK3[l][1]$	$TK1[l][2] \oplus TK2[l][2]$ $\oplus TK3[l][2]$	$TK1[l][3] \oplus TK2[l][3]$ $\oplus TK3[l][3]$
Round $i = 2$, $ETK_i[j, j = 0:15] = L_1(TK1[l]) \oplus L_2(TK2[l]) \oplus L_2(TK3[l])$, $l = 9, 15, 8, 13, 9, 15, 8, 13,$ $11, 10, 14, 12, 9, 15, 8, 13$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{2,3\}$ $\oplus TK3[l]\{1\}$	$TK1[l][1] \oplus TK2[l][0]$ $\oplus TK3[l]\{2\}$	$TK1[l][2] \oplus TK2[l][1]$ $\oplus TK3[l]\{3\}$	$TK1[l][3] \oplus TK2[l][2]$ $\oplus TK3[l]\{0,3\}$

Table 14. SKINNY-128-384 tweakey relations for round $i = 15, 16, \cdots, 21$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i = 15$, $TK_i[j, j = 0:7] = L_1^8(\mathit{TK1}[l]) \oplus L_2^8(\mathit{TK2}[l]) \oplus L_2^8(\mathit{TK3}[l])$, $l = 8, 9, 10, 11, 12, 13, 14, 15$ and Round $i = 16$, $TK_i[j, j = 0:7] = L_1^8(\mathit{TK1}[l]) \oplus L_2^8(\mathit{TK2}[l]) \oplus L_2^8(\mathit{TK3}[l])$, $l = 0, 1, 2, 3, 4, 5, 6, 7$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$\mathit{TK1}[l][0] \oplus \mathit{TK2}[l]\{0,4,6\}$ $\mathit{TK3}[l]\{0,6\}$	$\mathit{TK1}[l][1] \oplus \mathit{TK2}[l]\{1,5,7\}$ $\mathit{TK3}[l]\{1,7\}$	$\mathit{TK1}[l][2] \oplus \mathit{TK2}[l]\{0,2\}$ $\mathit{TK3}[l]\{0,2,6\}$	$\mathit{TK1}[l][3] \oplus \mathit{TK2}[l]\{1,3\}$ $\mathit{TK3}[l]\{1,3,7\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$\mathit{TK1}[l][4] \oplus \mathit{TK2}[l]\{2,4\}$ $\mathit{TK3}[l]\{0,2,4,6\}$	$\mathit{TK1}[l][5] \oplus \mathit{TK2}[l]\{3,5\}$ $\mathit{TK3}[l]\{1,3,5,7\}$	$\mathit{TK1}[l][6] \oplus \mathit{TK2}[l]\{4,6\}$ $\mathit{TK3}[l]\{0,2,4\}$	$\mathit{TK1}[l][7] \oplus \mathit{TK2}[l]\{5,7\}$ $\mathit{TK3}[l]\{1,3,5\}$
Round $i = 17$, $TK_i[j, j = 0:7] = L_1^9(\mathit{TK1}[l]) \oplus L_2^9(\mathit{TK2}[l]) \oplus L_2^9(\mathit{TK3}[l])$, $l = 9, 15, 8, 13, 10, 14, 12, 11$ and Round $i = 18$, $TK_i[j, j = 0:7] = L_1^9(\mathit{TK1}[l]) \oplus L_2^9(\mathit{TK2}[l]) \oplus L_2^9(\mathit{TK3}[l])$, $l = 1, 7, 0, 5, 2, 6, 4, 3$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$\mathit{TK1}[l][0] \oplus \mathit{TK2}[l]\{3,7\}$ $\mathit{TK3}[l]\{1,7\}$	$\mathit{TK1}[l][1] \oplus \mathit{TK2}[l]\{0,4,6\}$ $\mathit{TK3}[l]\{0,2,6\}$	$\mathit{TK1}[l][2] \oplus \mathit{TK2}[l]\{1,5,7\}$ $\mathit{TK3}[l]\{1,3,7\}$	$\mathit{TK1}[l][3] \oplus \mathit{TK2}[l]\{0,2\}$ $\mathit{TK3}[l]\{0,2,4,6\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$\mathit{TK1}[l][4] \oplus \mathit{TK2}[l]\{1,3\}$ $\mathit{TK3}[l]\{1,3,5,7\}$	$\mathit{TK1}[l][5] \oplus \mathit{TK2}[l]\{2,4\}$ $\mathit{TK3}[l]\{0,2,4\}$	$\mathit{TK1}[l][6] \oplus \mathit{TK2}[l]\{3,5\}$ $\mathit{TK3}[l]\{1,3,5\}$	$\mathit{TK1}[l][7] \oplus \mathit{TK2}[l]\{4,6\}$ $\mathit{TK3}[l]\{2,4,6\}$
Round $i = 19$, $TK_i[j, j = 0:7] = L_1^{10}(\mathit{TK1}[l]) \oplus L_2^{10}(\mathit{TK2}[l]) \oplus L_2^{10}(\mathit{TK3}[l])$, $l = 15, 11, 9, 14, 8, 12, 10, 13$ and Round $i = 20$, $TK_i[j, j = 0:7] = L_1^{10}(\mathit{TK1}[l]) \oplus L_2^{10}(\mathit{TK2}[l]) \oplus L_2^{10}(\mathit{TK3}[l])$, $l = 7, 3, 1, 6, 0, 4, 2, 5$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$\mathit{TK1}[l][0] \oplus \mathit{TK2}[l]\{2,6\}$ $\mathit{TK3}[l]\{0,2,6\}$	$\mathit{TK1}[l][1] \oplus \mathit{TK2}[l]\{3,7\}$ $\mathit{TK3}[l]\{1,3,7\}$	$\mathit{TK1}[l][2] \oplus \mathit{TK2}[l]\{0,4,6\}$ $\mathit{TK3}[l]\{0,2,4,6\}$	$\mathit{TK1}[l][3] \oplus \mathit{TK2}[l]\{1,5,7\}$ $\mathit{TK3}[l]\{1,3,5,7\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$\mathit{TK1}[l][4] \oplus \mathit{TK2}[l]\{0,2\}$ $\mathit{TK3}[l]\{0,2,4\}$	$\mathit{TK1}[l][5] \oplus \mathit{TK2}[l]\{1,3\}$ $\mathit{TK3}[l]\{1,3,5\}$	$\mathit{TK1}[l][6] \oplus \mathit{TK2}[l]\{2,4\}$ $\mathit{TK3}[l]\{2,4,6\}$	$\mathit{TK1}[l][7] \oplus \mathit{TK2}[l]\{3,5\}$ $\mathit{TK3}[l]\{3,5,7\}$
Round $i = 21$, $TK_i[j, j = 0:7] = L_1^{11}(\mathit{TK1}[l]) \oplus L_2^{11}(\mathit{TK2}[l]) \oplus L_2^{11}(\mathit{TK3}[l])$, $l = 11, 13, 15, 12, 9, 10, 8, 14$			
$TK_i[j][0]$	$TK_i[j][1]$	$TK_i[j][2]$	$TK_i[j][3]$
$\mathit{TK1}[l][0] \oplus \mathit{TK2}[l]\{1,5\}$ $\mathit{TK3}[l]\{1,3,7\}$	$\mathit{TK1}[l][1] \oplus \mathit{TK2}[l]\{2,6\}$ $\mathit{TK3}[l]\{0,2,4,6\}$	$\mathit{TK1}[l][2] \oplus \mathit{TK2}[l]\{3,7\}$ $\mathit{TK3}[l]\{1,3,5,7\}$	$\mathit{TK1}[l][3] \oplus \mathit{TK2}[l]\{0,4,6\}$ $\mathit{TK3}[l]\{0,2,4\}$
$TK_i[j][4]$	$TK_i[j][5]$	$TK_i[j][6]$	$TK_i[j][7]$
$\mathit{TK1}[l][4] \oplus \mathit{TK2}[l]\{1,5,7\}$ $\mathit{TK3}[l]\{1,3,5\}$	$\mathit{TK1}[l][5] \oplus \mathit{TK2}[l]\{0,2\}$ $\mathit{TK3}[l]\{2,4,6\}$	$\mathit{TK1}[l][6] \oplus \mathit{TK2}[l]\{1,3\}$ $\mathit{TK3}[l]\{3,5,7\}$	$\mathit{TK1}[l][7] \oplus \mathit{TK2}[l]\{2,4\}$ $\mathit{TK3}[l]\{0,4\}$

Table 15. SKINNY-128-384 equivlant tweakey relations for round $i = 1, 2$ ($L_1^h = P_T^h, L_2^h = (LFSR \circ P_T)^h$).

Round $i=1$, $ETK_i[j, j=0:15] = TK1[l] \oplus TK2[l] \oplus TK3[l]$, $l = 0,1,2,3,0,1,2,3,7,4,5,6,0,1,2,3$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l][0]$ $\oplus TK3[l][0]$	$TK1[l][1] \oplus TK2[l][1]$ $\oplus TK3[l][1]$	$TK1[l][2] \oplus TK2[l][2]$ $\oplus TK3[l][2]$	$TK1[l][3] \oplus TK2[l][3]$ $\oplus TK3[l][3]$
$ETK_i[j][4]$	$ETK_i[j][5]$	$ETK_i[j][6]$	$ETK_i[j][7]$
$TK1[l][4] \oplus TK2[l][4]$ $\oplus TK3[l][4]$	$TK1[l][5] \oplus TK2[l][5]$ $\oplus TK3[l][5]$	$TK1[l][6] \oplus TK2[l][6]$ $\oplus TK3[l][6]$	$TK1[l][7] \oplus TK2[l][7]$ $\oplus TK3[l][7]$
Round $i=2$, $ETK_i[j, j=0:15] = L_1(TK1[l]) \oplus L_2(TK2[l]) \oplus L_2(TK3[l])$, $l = 9,15,8,13,9,15,8,13,$ $11,10,14,12,9,15,8,13$			
$ETK_i[j][0]$	$ETK_i[j][1]$	$ETK_i[j][2]$	$ETK_i[j][3]$
$TK1[l][0] \oplus TK2[l]\{5,7\}$ $\oplus TK3[l][1]$	$TK1[l][1] \oplus TK2[l][0]$ $\oplus TK3[l][2]$	$TK1[l][2] \oplus TK2[l][1]$ $\oplus TK3[l][3]$	$TK1[l][3] \oplus TK2[l][2]$ $\oplus TK3[l][4]$
$ETK_i[j][4]$	$ETK_i[j][5]$	$ETK_i[j][6]$	$ETK_i[j][7]$
$TK1[l][4] \oplus TK2[l][3]$ $\oplus TK3[l][5]$	$TK1[l][5] \oplus TK2[l][4]$ $\oplus TK3[l][6]$	$TK1[l][6] \oplus TK2[l][5]$ $\oplus TK3[l][7]$	$TK1[l][7] \oplus TK2[l][6]$ $\oplus TK3[l]\{0,6\}$

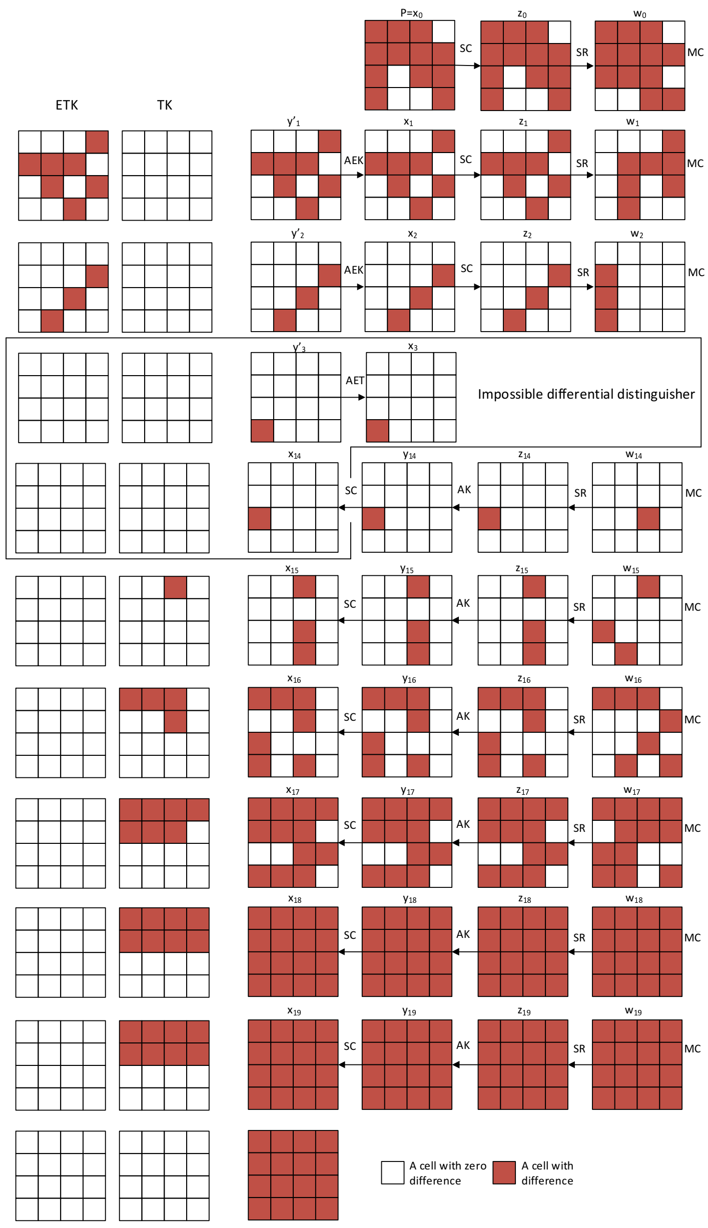

Fig. 4. Impossible differential attack on 20-round SKINNY-n-$2n$