Cryptanalysis of Reduced round SKINNY Block Cipher

Sadegh Sadeghi[1], Tahere Mohammadi[2] and Nasour Bagheri[2]

[1] Kharazmi University, Tehran, Iran, S.Sadeghi.Khu@gmail.com
[2] Shahid Rajaee Teacher Training University, Tehran, Iran,
t_mohammadi90@yahoo.com,Nbagheri@srttu.edu

Abstract. SKINNY is a family of lightweight tweakable block ciphers designed to have the smallest hardware footprint. In this paper, we present zero-correlation linear approximations and related-tweake impossible differential characteristics for different versions of SKINNY. We utilize meet-in-the-middle approach to construct 9-round and 10-round zero-correlation linear distinguisher. We also obtain 12-round related-tweakey impossible differential characteristics for both SKINNY-64 and 128 in TK1 model and TK2 model. To the best of our knowledge, the presented zero-correlation characteristics in this paper is the first investigation of the security of SKINNY against this attack.

Keywords: SKINNY · Zero-correlation linear cryptanalysis · Related-tweakey impossible differential cryptanalysis

1 Introduction

The SKINNY [2] lightweight tweakable block cipher is introduced to compete with NSA recent design SIMON [1] in terms of hardware/software performances. Designers of this block cipher investigated its security against well known attacks in the context such as linear and differential cryptanalysis [13, 5], impossible differential cryptanalysis [4], integral attack [7, 11] and etc. In this paper we search for zero-correlation linear extinguisher [6] and related-tweakey impossible differential characteristics [8] which are missing in the security analysis presented by designers.

1.1 Related Work.

Since SKINNY is a new designed block cipher, there is not much work done. Except the attacks applied by the designers, there are just two results presenting impossible differential cryptanalysis on SKINNY. In [12] the authors derived a 12-round related-tweakey impossible differential characteristic for SKINNY-64-64 (or 128-128) and obtained 18-round attack by key recovery. They also attacked 22 and 27 rounds of SKINNY-64-128 (or 128-265) and SKINNY-64-192 (or 128-384) respectively, by utilizing rectangle distinguishers. The authors of [15] utilized the 11-round impossible differential characteristic given in the main paper and presented 18, 20 and 22-round attack applying the key recovery attack for SKINNY-64-64 (or 128-128), SKINNY-64-128 (or 128-265) and SKINNY-64-192 (or 128-384) respectively. No results on the security of SKINNY against zero-correlation cryptanalysis are published yet.

1.2 Our Contribution.

The main purpose of this paper is to search related-tweakey impossible differential and zero-correlation linear characteristics on SKINNY. This paper proposes 9-round and 10-round distinguishers on all variants of SKINNY. All the zero-correlation linear characteristics are searched using Mixed-Integer Linear Programming (MILP). We also propose 12-round related-tweakey impossible differential distinguishers for SKINNY-64-64(or 128-128) and SKINNY-64-128. All related-tweakey impossible differential characteristics for SKINNY-64-64(or 128-128) are given based on MILP results.

1.3 Outline.

The remainder of this paper is organized as follows. Section 2 gives a brief description of SKINNY. Section 3 provides a general introduction of zero-correlation linear cryptanalysis and proposes zero-correlation linear distinguishers for different versions of SKINNY. Section 4 presents related-tweakey impossible characteristics of SKINNY. Finally, we conclude the paper in Section 5.

2 Preliminaries

In this section we give a brief description of SKINNY, its round function and key schedule.

2.1 A brief description of SKINNY

The lightweight block ciphers of the SKINNY family have 64-bit and 128-bit block versions. In both $n = 64$ and $n = 128$ versions (n is the block size), the internal state is viewed as a 4×4 square array of cells, where each cell can be a nibble (when $n = 64$) or a byte (when $n = 128$). SKINNY is built using the TWEAKEY framework [9] and there are three versions with tweakey sizes $t = n$, $t = 2n$ and $t = 3n$. For simplicity in writing, we show the SKINNY with block size n and tweakey size t with $SKINNY - n - t$.

Initialization The cipher takes a plaintext $m = m_0||m_1||\dots||m_{14}||m_{15}$, while the m_i are s-bit cells (we have $s = 4$ for the 64-bit block SKINNY versions and $s = 8$ for the 128-bit block SKINNY versions). the cipher's internal state is initialized as follows.

$$IS = \begin{pmatrix} m_0 & m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 & m_7 \\ m_8 & m_9 & m_{10} & m_{11} \\ m_{12} & m_{13} & m_{14} & m_{15} \end{pmatrix}$$

The Round Function One encryption round of SKINNY is composed of these five operations: SubCells, AddConstants, AddRoundTweakey, ShiftRows and MixColumns (illustration is in Figure 1).

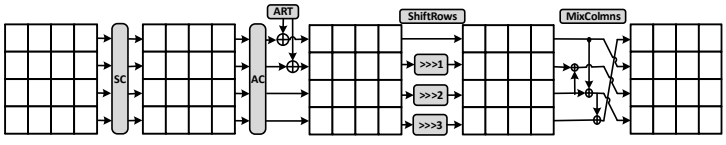

Figure 1: SKINNY round function

Table 1: The 4-bit S-box used in SKINNY-64 in hexadecimal form.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S_4[x]$	C	6	9	0	1	A	2	B	C	8	5	D	4	E	7	F

SubCells Each cell of the cipher internal state goes through an s-bit S-box. For $s = 4$ this s-box is shown in Table 1.

AddConstants In this step the round constants derived using a 6-bit LFSR are combined with the state.

AddRoundTweakey The first and second rows of all tweakey arrays are extracted and bitwise exclusive-ORed to the cipher internal state, respecting the array positioning. Then, the tweakey arrays are updated in 2 steps as shown in Figure 2. In the first step, the following permutation P_T is applied on tweakey array:

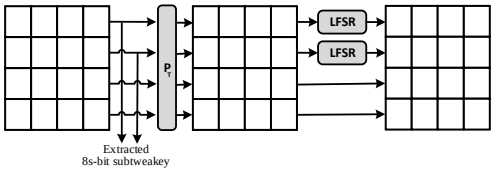

Figure 2: The TWEAKEY schedule of SKINNY

$$P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7].$$

In the second step, every cell of the first and second rows is individually updated with an LFSR as follows:

$$(x_3||x_2||x_1||x_0) \longrightarrow (x_2||x_1||x_0||x_3 \oplus x_2),$$

Note that, no LFSR is used in TK1 or single key case. More details about LFSRs for $s = 8$ and TK3 model is given in [**?**].

ShiftRows The second, third, and fourth cell rows are respectively rotated by 1, 2 and 3 positions to the right. This operation can be performed by applying a permutation P on the cells positions of the cipher internal state cell array.

$$P = [0, 1, 2, 3, 7, 4, 5, 6, 10, 11, 8, 9, 13, 14, 15, 12]$$

MixColumns Each column of the cipher internal state array is multiplied by a binary matrix M given below:

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

3 Zero-correlation cryptanalysis

As described in [14], we consider a n-bit block cipher with input variable $x \in F_2^n$, and f-function $f : F_2^n \longmapsto F_2^n$. If we call v and u as the input and output mask, respectively, the linear approximation is defined as follows:

$$x \longmapsto v.x \oplus u.f(x).$$

Its probability can be defined as:

$$p(v;u) = pr(v.x \oplus u.f(x) = 0),$$

and it has correlation of:

$$C_f(v;u) = 2p(v;u) - 1.$$

We note that the correlation of an approximation will be equal to zero if the probability of approximation is $\frac{1}{2}$.

In zero-correlation linear cryptanalysis, we look for a linear approximation with correlation zero for all keys. There are usually some XORs, F-functions and branches used in each round of any ciphers. According to [6] there are three rules for these operations:

Lemma 1. ***(XOR operation)*** *Either the three linear selection patterns at an XOR $\oplus$ are equal or the correlation over $\oplus$ is exactly 0*

Lemma 2. ***(Branching operation)*** *Either the three linear selection patterns at a branching point $\bullet$ sum up to 0 or the correlation over $\bullet$ is exactly 0.*

Lemma 3. ***(Permutation approximation)*** *Over a permutation ϕ, if the input and output selection patterns are neither both zero nor both nonzero, the correlation over ϕ is exactly zero.*

3.1 Zero-correlation Linear distinguishers of SKINNY

In this section, we use "0" to denote a zero mask, Γ^i to denote a nonzero mask in $i-th$ cell ($i = 0, \ldots, 15$) and "?" to denote a zero or nonzero mask. Also we use $\Gamma^i_{in} \overset{r}{\nrightarrow} \Gamma^j_{out}$ to show the correlation of linear approximation of r-round SKINNY with input mask Γ^i_{in} ($i-$th cell of input) and output mask Γ^j_{out} ($j-$th cell of output) is zero.

3.2 9-round Zero-correlation linear distinguishers for SKINNY

We searched for zero-correlation characteristics with the miss-in-the-middle technique. For the 9-round distinguisher we list all the zero-correlation linear approximations at Table 2. Based on this table there are 172 different characteristics with single active cells in input and output masks. For the 9-round distinguisher one of the 172 zero-correlation linear

Table 2: Zero-correlation linear approximations $\Gamma^i_{in} \overset{r}{\nrightarrow} \Gamma^j_{out}$ for 9-round SKINNY.

r	NO.	Zero-correlation linear approximations
9	172	if $i = 0, 1, 2, 3$, then $j = 0, 1, \ldots, 15$ if $i = 4, 5, 6, 7$, then $j = 4, 5, 6, 7$ if $i = 8$, then $j = 4, \ldots, 11, 13, 14, 15$ if $i = 9$, then $j = 4, \ldots, 12, 14, 15$ if $i = 10$, then $j = 4, \ldots, 13, 15$ if $i = 11$, then $j = 4, \ldots, 14$ if $i = 12, 13, 14, 15$, then $j = 4, \ldots, 15$

characteristics is as follows

$$(\Gamma^{15}_{in}) \overset{9}{\nrightarrow} (\Gamma^{12}_{out}).$$

As can be seen in Figure 3, in the encryption direction,we find that for any 4-round non-zero linear characteristic with input mask of (Γ^{15}_{in}), the linear mask of the internal state must be

$$(0, 0, \Gamma^2, \Gamma^3, ?, \Gamma^5, \Gamma^6, 0, \Gamma^8, 0, \Gamma^{10}, 0, \Gamma^{12}, \Gamma^{13}, ?, \Gamma^{15}). \quad (1)$$

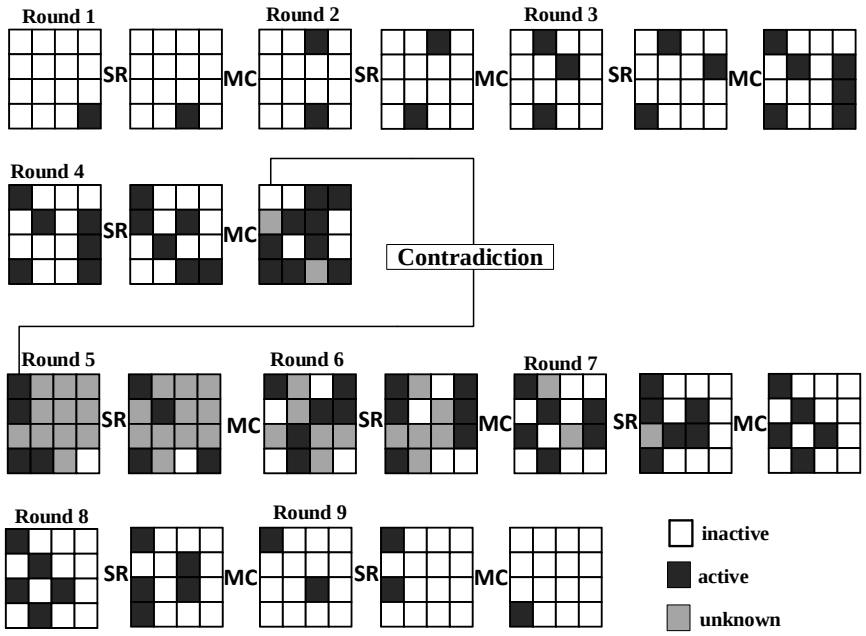

Figure 3: The 9-round distinguisher for SKINNY in single key model. SR and MC stand for ShiftRows and MixColumns, respectively. SubCel, AddConstant and AddRoundTweakey are omitted since they are not related here.

Similarly, in the decryption direction for any 7-round non-zero linear characteristic with output mask of Γ^{12}_{out}, the linear mask of the internal state must be

$$(\Gamma^0, ?, ?, ?, \Gamma^4, ?, ?, ?, ?, ?, ?, ?, \Gamma^{12}, \Gamma^{13}, ?, 0). \tag{2}$$

If we combine (1) and (2) with each other we derive a 9-round zero correlation linear distinguisher for SKINNY.

3.3 10-round Zero-correlation linear distinguishers for SKINNY

For the 10-round distinguisher, 16 different characteristics with single active cells in input and output masks have been found which are as follows

$$(\Gamma^i_{in} \overset{10}{\nrightarrow} \Gamma^j_{out}) \qquad \text{if} \quad i = 0, 1, 2, 3 \quad \text{then} \quad j = 4, 5, 6, 7.$$

For example one of 10-round zero-correlation linear characteristics is as follows

$$(\Gamma^0_{in}) \overset{10}{\nrightarrow} (\Gamma^4_{out}),$$

to obtain this characteristic, we can not directly reach to any contradictions for 10-round by using miss-in-the-middle technique. Therefore, we firstly construct a 9-round zero-correlation distinguisher as shown in Figure 4. This distinguisher consists of a forward part (along the encryption direction) and a backward part (along the decryption direction). After encrypting 4 rounds in the forward part and 5 rounds in the backward part a contradiction will happen in the first cell of the middle state which it is shown in Figure 4.

By decrypting (or encrypting) 1 more round in the backward part (or forward part), no contradiction will be found; but from the forward part, we know that the 7th and 10th

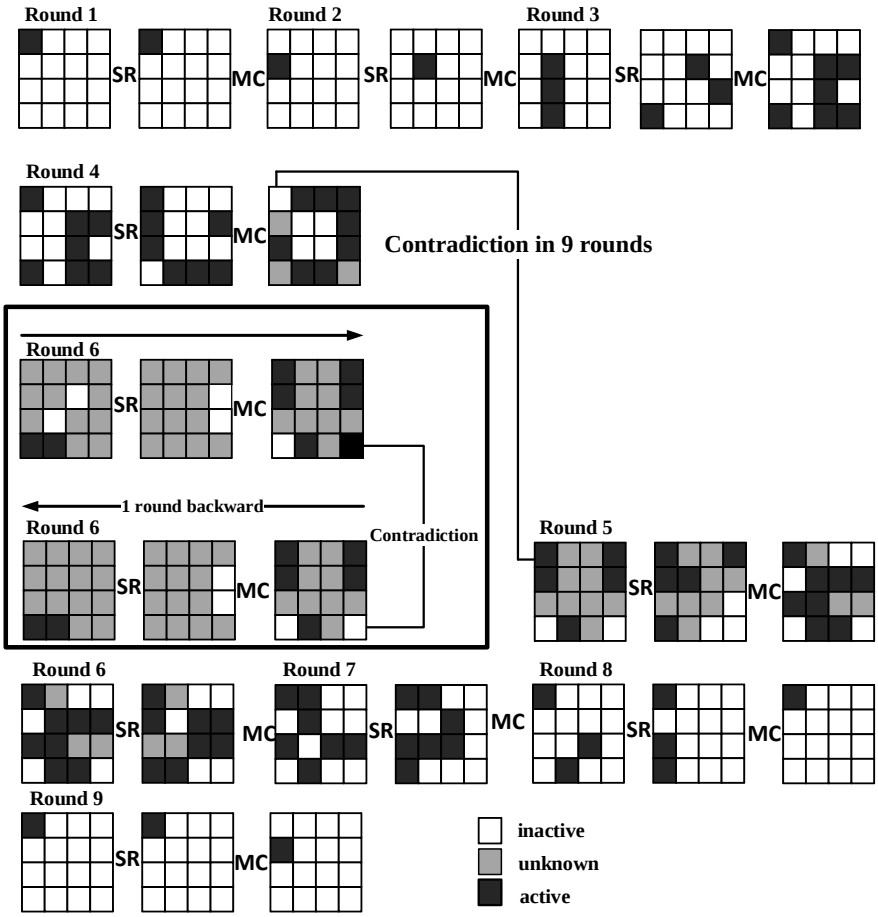

Figure 4: Zero correlation characteristic for 9-round (extended to 10-round) SKINNY in single key model. SR and MC stand for ShiftRows and MixColumns, respectively. Subcells, AddConstant and AddTweakey are omitted since they are not related here.

cells of the output mask of this new decrypted round must be inactive. Now, we show that if these cells be inactive, we will reach another contradiction. To this end, we consume these two cells inactive and by encrypting one round in the backward part, we see that in this case the 15th cells of the input mask of this new round (6th round) will change and becomes active and this is a contradiction. The more details are depicted in Figure 4.

4 Related-tweakey Impossible Differential characteristics of SKINNY

The impossible differential attack, which was independently proposed by Bi- ham et al. [4] and Knudsen [10], is one of the most popular cryptanalytic tools for block ciphers. impossible differential cryptanalysis starts with finding an input difference which results in an output difference with probability 0. Related-tweakey attacks [3] let a cryptanalyst to choose appropriate relation between keys and then to predict the encryptions under these keys. Related-tweakey impossible differential attack [8] is a combination of the two aforesaid attacks.

In this section, we describe a related-tweakey impossible differential attack on the

reduced-round SKINNY block cipher. We obtain 12-round related-tweakey impossible differential characteristics with TK1 and TK2 model. To this end, we firstly introduce some notations: we use "0" to denote a zero difference, Δ^i to denote a nonzero difference in $i-th$ cell ($i=0,\ldots,15$), Δ^i_j to denote the XOR difference of the $j-th$ bit of the $i-th$ cell ($j=0,1,2,3$ and $i=0,\ldots,15$) and "?" to denote a zero or nonzero difference.

In [**?**], the miss-in-the-middle approach was used to find 11-round impossible differential characteristic on SKINNY as follows

$$(0,0,0,0,0,0,0,0,0,0,0,\Delta^{12},0,0,0) \overset{11}{\nrightarrow} (0,0,0,0,0,0,0,0,\Delta^{8},0,0,0,0,0,0,0). \quad (3)$$

Then they have utilized it to attack 16-round SKINNY-64-64 (or 128-128) tweakey and 18-round SKINNY-64-128. In this paper, in order to find related-tweakey impossible differential characteristic, we use miss-in-the-middle approach to find 12-round related-tweakey impossible differentials for SKINNY.

4.1 Searching Related-tweakey Impossible Differential characteristics on SKINNY in TK1 model

We found that the longest Related-tweakey impossible differential characteristics when only one cell is active in the input and output differences reach 12 rounds. We listed all the related-tweakey impossible differential characteristics in Table 3. Based on this table there are 100 truncated impossible differential characteristics under TK1 model with single active cell in both input and output and also input of TK1.

Table 3: Truncated Related-tweakey impossible differential characteristics $\big(\Delta(input),\Delta(TK1),\Delta(output)\big)$ for 12-round SKINNY.

r	NO.	Related-tweakey impossible differential
12	100	(1,9,13),(1,10,15),(1,11,11),(2,8,8) (3,9,13),(4,8,8),(4,10,15),(5,9,13) (6,9,13),(6,10,15),(7,10,15),(7,11,11) (12,8,8),(12,9,13),(12,10,15),(12,11,11) (13,9,13),(13,10,15),(14,9,13),(14,10,15) (14,11,11),(15,8,8),(15,9,13),(15,10,15) (15,11,11)

For example if we choose the input difference to be

$$\big(\Delta(input);\Delta(TK1)\big) = \big((0,\ldots,0,\Delta^{12},0,0,0);(0,\ldots,0,\Delta^{8},0,0,0,0,0,0,0)\big),$$

which $\Delta(TK1)$ denotes the input related key differences of TK1, then after 5 rounds, the truncated output related-tweakey impossible difference should have the following form

$$(?,?,?,?,0,?,?,\Delta^{7},0,\Delta^{9},?,?,\Delta^{12},?,?,?) \quad (4)$$

Likewise, if we choose the output difference $(0,\ldots,0,\Delta^{8},0,0,0,0,0,0,0)$, then after propagating backwards for 7 rounds, the truncated output related-tweakey impossible difference should be in the following form

$$(?,\Delta^{1},\Delta^{2},?,?,?,?,?,\Delta^{8},?,?,?,0,0,\Delta^{14},\Delta^{15}) \quad (5)$$

With combining (4) and (5) , we can derive a 12-round related-tweakey impossible differential characteristic as follows (also depicted in Figure 6):

$$\underbrace{(0,\ldots,0,\Delta^{12},0,0,0;}_{\Delta(input)}\underbrace{0,\ldots,0,\Delta^{8},0,0,0,0,0,0,0)}_{\Delta(TK1)} \overset{12R}{\nrightarrow} \underbrace{(0,\ldots,0,\Delta^{8},0,0,0,0,0,0,0)}_{\Delta(output),} \quad (6)$$

4.2 Searching Related-tweakey Impossible Differential characteristics on SKINNY in TK2 model

In previous section, we presented miss-in-the-middle technique to search related-tweakey impossible differential characteristic using nibble-based (or byte-based) property. In this section, we obtain 12-round related-tweakey impossible differential characteristics using bit-based property on SKINNY-64 in the TK2 model (i.e both TK1 and TK2 are considered).We obtain the 12-round related-tweakey impossible differential (see Figure 7). More specifically, this distinguisher consists of two parts: encryption direction (forward) and decryption direction (backward). For the encryption direction, we find that for any 5-round non-zero related-tweakey impossible differential with input difference being

$$\underbrace{(0,\ldots,0,\Delta_0^{12},0,0,0}_{\Delta(input)};\underbrace{0,\ldots,0,\Delta_2^{8},0,0,0,0,0,0,0}_{\Delta(TK1)};\underbrace{0,\ldots,0,\Delta_2^{8},0,0,0,0,0,0,0)}_{\Delta(TK2),}$$

the truncated output related-tweakey impossible difference must be

$$(?,?,?,?,0,?,?,\Delta^7,?,\Delta^9,?,?,\Delta^{12},?,?,?).$$

As to the decryption direction, we observe that for any 7-round non-zero related-tweakey impossible differential with input difference being

$$\underbrace{(0,\ldots,0,\Delta_0^{8},0,0,0,0,0,0,0)}_{\Delta(output)}$$

the truncated output related-tweakey impossible difference must be

$$(?,?,\Delta^2,\Delta^3,0,?,?,?,?,?,0,?,\Delta^{11},\Delta^{12},\Delta^{13},\Delta^{14},0).$$

Combining the above two parts, we can obtain a 12-round related-tweakey impossible differential for SKINNY in TK2 model.

5 Conclusion

In this work we presented zero-correlation linear and related-tweakey impossible differential characteristics on SKINNY block cipher. We were able to construct 9-round and 10-round zero-correlation linear distinguishers for both SKINNY-64 and 128 versions based on the miss-in-the-middle technique. Moreover, we searched all zero-correlation linear characteristics using MILP technique. We have also proposed all 12-round related-tweakey impossible differential characteristics of SKINNY-64-64 (or 128-128). In addition, we found a 12-round related-tweakey impossible characteristic for SKINNY-64-128 based on bits, instead of nibbles or bytes. Based on MILP results, we claim the given characteristics are the longest with assumption of having single active cells in input and output masks (and tweakeys in related-tweakey cases).

References

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The simon and speck lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference*, page 175. ACM, 2015.

[2] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim. The skinny family of block ciphers and its low-latency variant mantis. In *Annual Cryptology Conference*, pages 123–153. Springer, 2016.

[3] E. Biham. New types of cryptanalytic attacks using related keys. *Journal of Cryptology*, 7(4):229–246, 1994.

[4] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 12–23. Springer, 1999.

[5] E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

[6] A. Bogdanov and V. Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Designs, codes and cryptography*, 70(3):369–383, 2014.

[7] J. Daemen, L. Knudsen, and V. Rijmen. The block cipher square. In *International Workshop on Fast Software Encryption*, pages 149–165. Springer, 1997.

[8] G. Jakimoski and Y. Desmedt. Related-key differential cryptanalysis of 192-bit key aes variants. In *International Workshop on Selected Areas in Cryptography*, pages 208–221. Springer, 2003.

[9] J. Jean, I. Nikolić, and T. Peyrin. Tweaks and keys for block ciphers: the tweakey framework. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 274–288. Springer, 2014.

[10] L. Knudsen. Deal-a 128-bit block cipher. *complexity*, 258(2):216, 1998.

[11] L. Knudsen and D. Wagner. Integral cryptanalysis. In *International Workshop on Fast Software Encryption*, pages 112–127. Springer, 2002.

[12] G. Liu, M. Ghosh, and S. Ling. Security analysis of skinny under related-tweakey settings. Cryptology ePrint Archive, Report 2016/1108, 2016. http://eprint.iacr.org/2016/1108.

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

[14] H. Soleimany and K. Nyberg. Zero-correlation linear cryptanalysis of reduced-round lblock. *Designs, Codes and Cryptography*, 73(2):683–698, 2014.

[15] M. Tolba, A. Abdelkhalek, and A. M. Youssef. Impossible differential cryptanalysis of skinny. Cryptology ePrint Archive, Report 2016/1115, 2016. http://eprint.iacr.org/2016/1115.

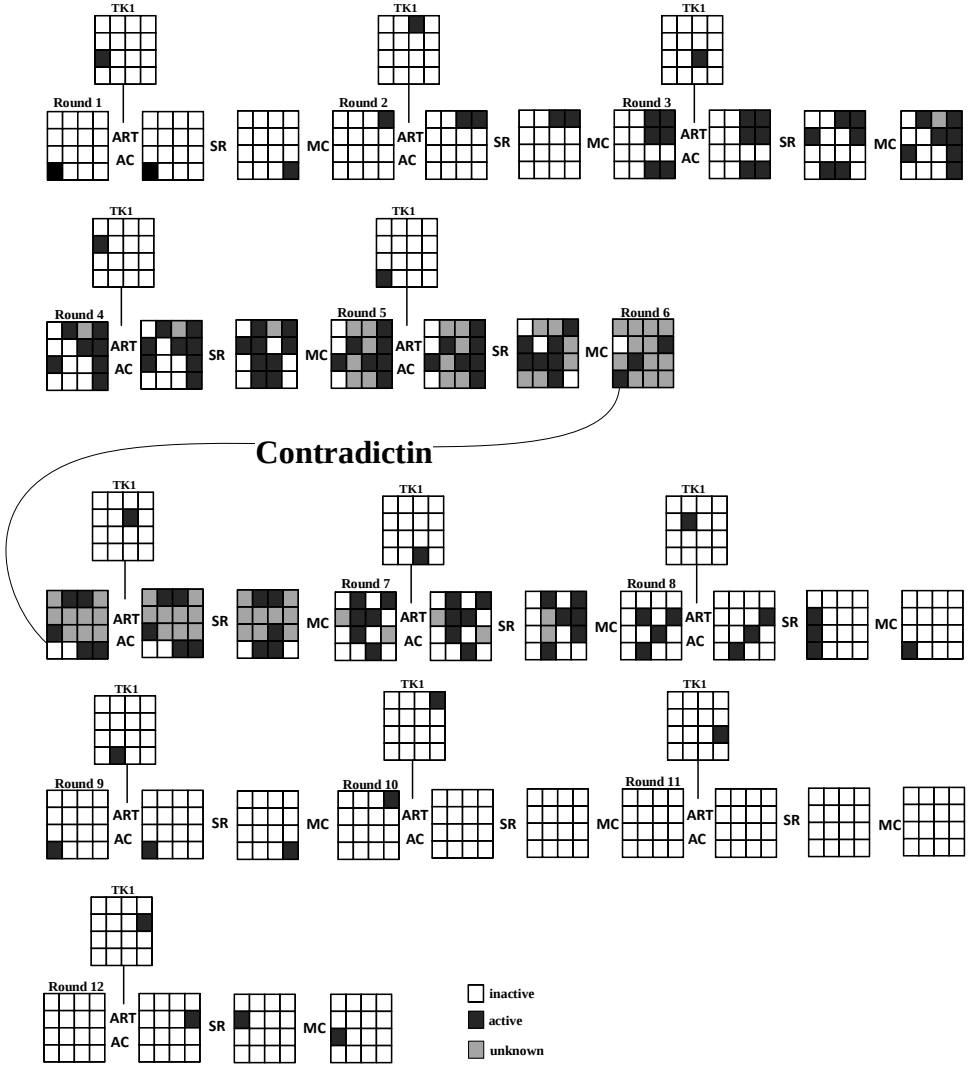

Figure 5: Related-tweakey impossible differential characteristic for 12-round SKINNY in TK1 model. ART, SR and MC stand for AddRoundTweakey, ShiftRows and MixColumns, respectively. SubCells and AddConstant are omitted since they are not related here.

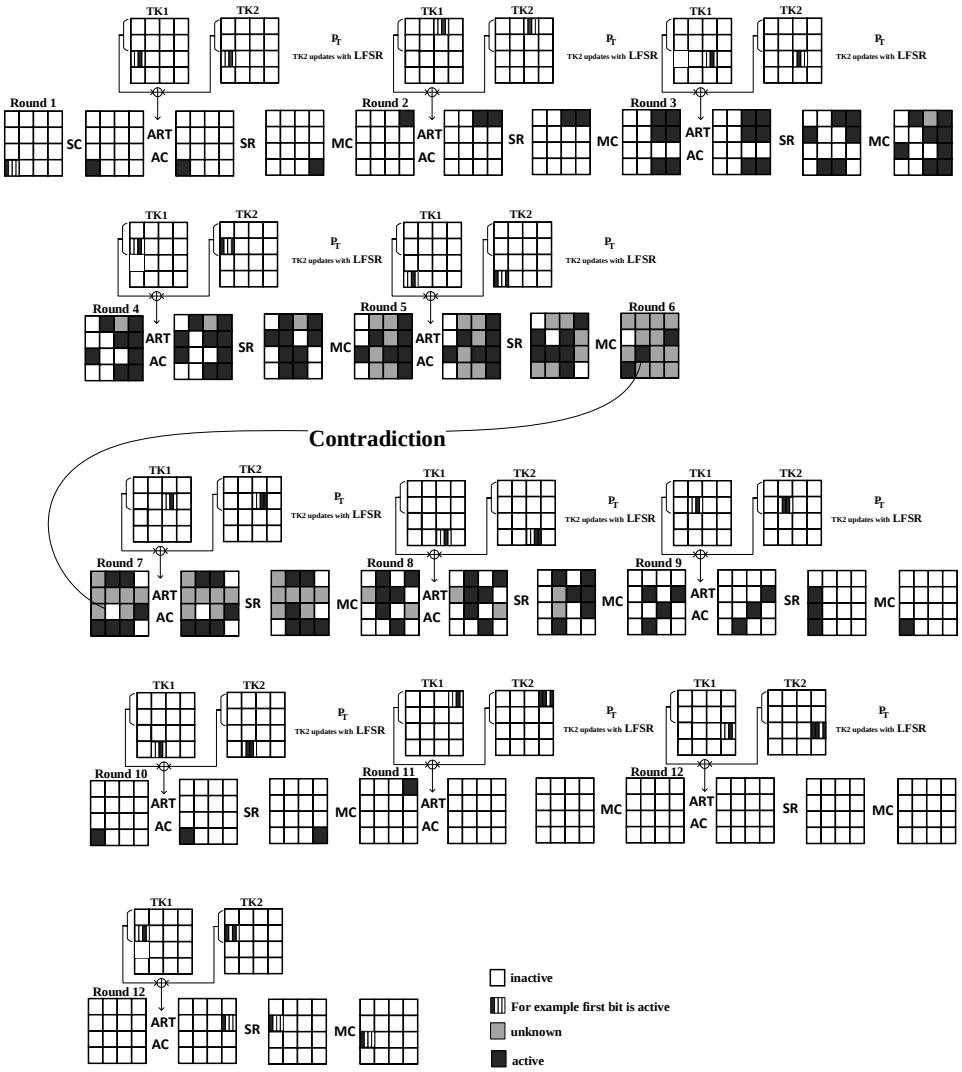

Figure 6: Related-tweakey impossible differential characteristic for 12-round SKINNY in TK2 model. SC, ART, SR and MC stand for SubCell, AddRoundTweakey, ShiftRows and MixColumns, respectively. AddConstant are omitted since they are not related here.