Investigation of the Optimal Linear Characteristics of BAKSHEESH (Full Version)

Yuxuan Peng[1,2,3], Jinpeng Liu[1,2], and Ling Sun(✉)[1,2,4]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China
[2] School of Cyber Science and Technology, Shandong University, Qingdao, China
[3] Institut Polytechnique de Paris, Palaiseau, France
[4] Quan Cheng Shandong Laboratory, Jinan, China
lingsun@sdu.edu.cn

Abstract. This paper aims to provide a more comprehensive understanding of the optimal linear characteristics of BAKSHEESH. Initially, an explicit formula for the absolute correlation of the R-round optimal linear characteristic of BAKSHEESH is proposed when $R \geqslant 12$. By examining the linear characteristics of BAKSHEESH with three active S-boxes per round, we derive some properties of the three active S-boxes in each round. Furthermore, we demonstrate that there is only one 1-round iterative linear characteristic with three active S-boxes. Since the 1-round linear characteristic is unique, it must be included in any R-round ($R \geqslant 12$) linear characteristics of BAKSHEESH with three active S-boxes per round. Finally, we confirm that BAKSHEESH's total number of R-round optimal linear characteristics is 3072 for $R \geqslant 12$. All of these characteristics are generated by employing the 1-round iterative linear characteristic.

Keywords: Linear cryptanalysis · Linear characteristic · BAKSHEESH.

1 Introduction

The evolution of lightweight cryptography has been influenced by the increased deployment of tiny computing devices and the advent of the Internet of Things (IoT). Resource-constrained devices, such as embedded systems, sensor networks, and RFID tags, have limited storage capacity, computing capabilities, and battery power. Existing encryption standards, such as AES [13], perform inefficiently on these devices. Researchers have been devising lightweight cryptography for resource-constrained devices to address this issue and have proposed a series of lightweight ciphers [3,5,6,8,9,11,14]. Some lightweight primitives, including PRESENT [8], PHOTON [10], and SPONGENT [7], have already been incorporated into ISO/IEC standards (ISO/IEC 29192-2:2012 and ISO/IEC 29192-5:2016).

Among the initially published lightweight encryption algorithms, PRESENT has been the subject of extensive analysis over the past decades. While PRESENT

maintains an elegant design, it has yet to benefit from current research developments. Consequently, Banik *et al.* [4] reevaluate the design strategy of PRESENT and introduce GIFT, a lightweight block cipher that outperforms PRESENT in terms of both security and efficiency. GIFT is a highly versatile cipher that exceeds many lightweight designs and remains a competitive option today, owing to its natural bitslice organisation of the inner data flow and its simplicity.

Following the main design philosophy of GIFT, Baksi *et al.* [2] suggested a new lightweight block cipher called `BAKSHEESH`. `BAKSHEESH` comprises 35 rounds, 12.50 per cent less than GIFT-128, while preserving the same security claims against classical attacks. Unlike the half-round key XOR in GIFT, `BAKSHEESH` employs the full-round key XOR, inspired by the DFA-resistant cipher DEFAULT [1]. Additionally, `BAKSHEESH` has reduced the cost of DEFAULT. These factors sparked our curiosity about `BAKSHEESH`.

`BAKSHEESH`'s designers established a lower bound on the number of active S-boxes for linear characteristics, ranging from one to 22 rounds. The bound grows by three every round, beginning with the twelfth round. In addition, the designers provided a linear characteristic with 22 rounds, specifically activating three S-boxes in each of the first 21 rounds. These observations heighten our motivation to examine the linear characteristics of `BAKSHEESH`, which extends over twelve rounds and contains three active S-boxes per round.

1.1 Our Findings

Motivated by observations about the linear characteristics of `BAKSHEESH`, our goal is to furnish more comprehensive information regarding the optimal linear characteristics of the cipher. The paper's findings can be summarised as follows.

Explicit formula for the absolute correlation of the optimal linear characteristics. We propose an explicit formula for the absolute correlation of `BAKSHEESH`'s optimal characteristics. Precisely, the absolute correlation $\mathrm{Cor}(R)$ of R-round optimal linear characteristics of `BAKSHEESH` with $R \geqslant 12$ can be calculated as $\mathrm{Cor}(R) = 2^{-3 \cdot R+2}$.

Positions of nonzero nibbles in linear masks of all optimal linear characteristics. We show that when using the nibble-oriented description of the round function, an R-round ($R \geqslant 12$) linear characteristic of `BAKSHEESH` with three nonzero nibbles in the input mask per round always positions two nonzero nibbles in the same column of the matrix state, and the final nonzero nibble is located in a different column. This discovery provides us with the initial information regarding all of `BAKSHEESH`'s optimal linear characteristics.

Uniqueness of a 1-round iterative linear characteristic with three active S-boxes. After studying the precise placements, concrete values, and other features of nonzero nibbles in linear masks, we demonstrate that there is only one 1-round iterative linear characteristic with three active S-boxes. Additionally, we show that any R-round ($R \geqslant 12$) linear characteristics of `BAKSHEESH` with three active S-boxes per round must include this 1-round characteristic due to its uniqueness.

Enumerating all R-round ($R \geqslant 12$) optimal linear characteristics. We demonstrate that the number of all R-round optimal linear characteristics of `BAKSHEESH` is 3072 when $R \geqslant 12$. Furthermore, the 1-round iterative linear characteristic is employed to generate all of `BAKSHEESH`'s R-round optimal linear characteristics. The automatic tool in [16] is used to verify the theoretical result.

Outline. Linear cryptanalysis and the target cipher `BAKSHEESH` are reviewed in Section 2. Section 3 offers a few observations regarding the linear properties of `BAKSHEESH`. Section 4 examines the positions of nonzero nibbles in linear masks for the linear characteristics of `BAKSHEESH`, which has three active S-boxes within each round. The precise positions, concrete values, and other details of the three nonzero nibbles in each round are elucidated in Section 5. In Section 6, we generate all R-round ($R \geqslant 12$) optimal linear characteristics of `BAKSHEESH` using the results from Sections 4 and 5. The paper is concluded in Section 7.

2 Preliminary

2.1 Linear Cryptanalysis

Linear cryptanalysis [12] is a known-plaintext attack on block ciphers. Matsui introduced it as an attack on the Data Encryption Standard (DES) [5]. The primary objective of linear cryptanalysis is to identify an r-round *linear approximation* (α, β) with a *bias*

$$\varepsilon(\alpha, \beta) = \frac{\{x \in \mathbb{F}_2^n | \alpha \cdot x \oplus \beta \cdot E_k(x) = 0\}}{2^n} - 0.5$$

distinct from zero for a given iterated block cipher E_k with an n-bit block size. α is the *input mask*, and β is the *output mask*. The effectiveness of the linear approximation increases with the absolute value of the bias. The *correlation* is a measure closely associated with the bias, calculated as

$$\mathrm{Cor}(\alpha, \beta) = 2 \cdot \varepsilon(\alpha, \beta).$$

The absolute value of the correlation $|\mathrm{Cor}(\alpha, \beta)|$ is called the *absolute correlation*.

Directly identifying lengthy and effective linear approximations is typically challenging due to the large state of modern block ciphers. Consequently, the most frequently employed approach is to identify suitable linear approximations (α_i, α_{i+1}) for each round function f_i $(0 \leqslant i \leqslant R-1)$ and connect these one-round linear approximations end-to-end to generate an R-round *linear characteristic* $(\alpha_0, \alpha_1, \ldots, \alpha_R)$. As per the piling-up lemma [12], the bias of the linear characteristic can be determined as

$$\varepsilon(\alpha_0, \alpha_1, \ldots, \alpha_R) = 2^{R-1} \prod_{i=0}^{R-1} \varepsilon(\alpha_i, \alpha_{i+1}).$$

When examining linear approximations for round functions, S-boxes are typically the most complex element. Given that they are the sole nonlinear operation

in the round function in most cases, the propagation of linear masks for them is non-deterministic. We typically create a table known as the *Linear Approximation Table* (LAT) to facilitate the analysis of S-boxes. The LAT of an s-bit S-box S is a table with 2^s rows and 2^s columns. The value

$$\#\{x \in \mathbb{F}_2^s | i \cdot x \oplus j \cdot S(x) = 0\} - 2^{s-1}, \quad 0 \leqslant i, j \leqslant 2^s - 1,$$

is stored in the i-th row and j-th column. The corresponding linear approximations for elements in LAT with nonzero values are called *possible* linear approximations. These linear approximations can be employed to develop linear characteristics for the objective ciphers. The S-box is *active* if the linear approximation of the S-box is possible and the absolute correlation is less than one. An *inactive* S-box is an S-box that has an absolute value of one for the correlation of the linear approximation.

Table 1. `BAKSHEESH`'s S-box in hexadecimal representation.

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

Table 2. P_{128} of `BAKSHEESH`.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{128}(i)$	96	65	34	3	64	33	2	99	32	1	98	67	0	97	66	35
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_{128}(i)$	100	69	38	7	68	37	6	103	36	5	102	71	4	101	70	39
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{128}(i)$	104	73	42	11	72	41	10	107	40	9	106	75	8	105	74	43
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{128}(i)$	108	77	46	15	76	45	14	111	44	13	110	79	12	109	78	47
i	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
$P_{128}(i)$	112	81	50	19	80	49	18	115	48	17	114	83	16	113	82	51
i	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
$P_{128}(i)$	116	85	54	23	84	53	22	119	52	21	118	87	20	117	86	55
i	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
$P_{128}(i)$	120	89	58	27	88	57	26	123	56	25	122	91	24	121	90	59
i	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
$P_{128}(i)$	124	93	62	31	92	61	30	127	60	29	126	95	28	125	94	63

2.2 Specification of `BAKSHEESH`

`BAKSHEESH` [2] is a 35-round lightweight block cipher that improves upon the famous cipher `GIFT-128` [4]. It receives a 128-bit plaintext $b_0\|b_1\|\cdots\|b_{127}$ as the

state, where b_0 is the most significant bit. The state can also be represented as $w_0\|w_1\|\cdots\|w_{31}$, where $w_i = b_{4i}\|b_{4i+1}\|b_{4i+2}\|b_{4i+3}$ for all $0 \leqslant i \leqslant 31$. The round function, illustrated in Figure 1, of BAKSHEESH, consists of the following steps.

`SubCells (SC)` The 4-bit S-box in Table 1 is employed in this operation, and it is applied to each nibble w_i of the state.

`PermBits (PB)` Table 2 supplies the bit permutation P_{128} engaged in BAKSHEESH. This operation transfers the bit from the bit location i of the internal state to the bit location $P_{128}(i)$ for all $0 \leqslant i \leqslant 127$. The four output bits of the same S-box in the current round must be delivered to the inputs of four distinct S-boxes in the subsequent round.

`AddConstants (AC)` **and** `AddRoundKey (AK)` This step involves adding the round key and the round constant. Given that the round keys and round constants do not influence the analysis in the following, we will refrain from providing further details. See Baksi *et al.* [2] for additional details.

Remark 1. The designers have provided a reference software implementation of BAKSHEESH, which can be accessed at https://github.com/anubhab001/baksheesh/. We verified this implementation and found that the source code includes a reverse permutation π on the 32 nibbles before and after the bit permutation applied on the state. π operates as $\pi(b_{4i}\|b_{4i+1}\|b_{4i+2}\|b_{4i+3}) = b_{4i+3}\|b_{4i+2}\|b_{4i+1}\|b_{4i}$. Consequently, the genuine bit permutation employed in BAKSHEESH should be the combination of the one in [2] and 64 4-bit permutations π, which is identical to the bit permutation P_{128} in Table 2. It explains the discrepancy between P_{128} in Table 2 and the one in [2]. The permutation π also affects the bit positions involved in the `AddConstants` operation, as illustrated in Figure 1. In order to convince the reader, the Supplementary Material[5] includes the encryption code for BAKSHEESH, which is implemented with the bit permutation P_{128} in Table 2. Our encryption code can pass the verification process with all of the test vectors offered by the designers [2].

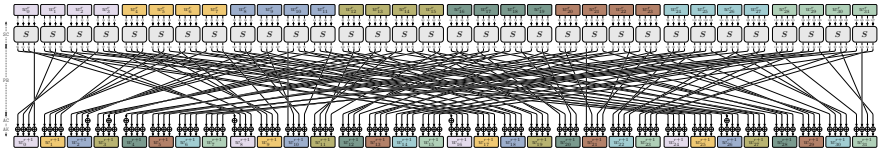


Fig. 1. Round function of BAKSHEESH.

2.3 Alternative Descriptions for the Round Function of BAKSHEESH

As demonstrated in [15], alternative descriptions exist for the round function of GIFT-128 [4]. Also, alternative descriptions for the round function of BAKSHEESH

[5] The Supplementary Material can be found at https://github.com/SunLing134340/Supplementary_Material_BAKSHEESH

can be created due to the similarity between the round functions of `GIFT-128` and `BAKSHEESH`. The descriptions will facilitate our investigation of the linear characteristics of `BAKSHEESH`.

The `PermBits` operation is the sole distinction between the standard description and the *bit-oriented description* of the round function of `BAKSHEESH`, as depicted in Figure 2(a). To be more precise, the `PermBits` operation is divided into the following `GroupMaps` and `TransNibbles` operations.

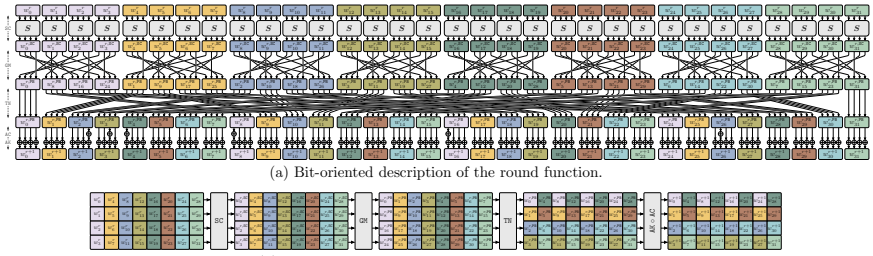
`GroupMaps (GM)` This operation employs a 16-bit permutation P_{16}, where

$$P_{16} = (12, 9, 6, 3,\ 8, 5, 2, 15,\ 4, 1, 14, 11,\ 0, 13, 10, 7).$$

P_{16} is applied to each of the 16-bit words $w_{4i}^{r,\mathtt{SC}} \| w_{4i+1}^{r,\mathtt{SC}} \| w_{4i+2}^{r,\mathtt{SC}} \| w_{4i+3}^{r,\mathtt{SC}}$ independently, where $w_{*}^{r,\mathtt{SC}}$ signifies the nibbles at the output of the `SubCells` operation in the r-th round.

`TransNibbles (TN)` This process moves the nibble from position i of the cipher state to position $T(i)$ for all $0 \leqslant i \leqslant 31$. $T(i)$ is calculated as

$$T(i) = 8 \cdot (i \bmod 4) + \lfloor i/4 \rfloor, \quad 0 \leqslant i \leqslant 31.$$



(a) Bit-oriented description of the round function.

(b) Nibble-oriented description of the round function.

Fig. 2. Alternative descriptions of the round function of `BAKSHEESH`.

Alternatively, the bit-oriented form in Figure 2(a) can be replaced with a nibble-oriented one, as shown in Figure 2(b), by rearranging the cipher state as a 4×8 matrix of nibbles. The subsequent properties of the permutations P_{16} and `TN` will be beneficial in analysing `BAKSHEESH`'s linear characteristics.

Property 1. *The permutation P_{16} sends four bits from the same input nibble to four distinct nibbles in the output.*

Property 2. *The `TN` operation transmits the four nibbles from the same column of the matrix state to four nibbles in four distinct columns.*

Property 3. *It is assumed that the input of the `TN` operation contains two nonzero nibbles, with one of the nibbles situated in the matrix's first four columns and the other in the last four columns. In the output of the `TN` operation, the two nonzero nibbles must be positioned in two distinct columns.*

3 Observations on Linear Properties of BAKSHEESH

Table 3 provides the LAT for the S-box of BAKSHEESH. It can be seen that all linear approximations with input and output masks having a Hamming weight of one are impossible. Given the property of the PB or GM operation, it is clear that any linear characteristics of BAKSHEESH that extend beyond three rounds are unable to activate a single S-box per round.

The designers of BAKSHEESH provided the upper bound on the absolute correlation for linear characteristics from one round to 22 rounds. Given that the absolute correlations of all feasible linear approximations for the S-box are equal to 2^{-1}, as listed in Table 3, the upper bound on the absolute correlation can be equivalently transformed into the lower bound on the number of linear active S-boxes. As illustrated in Figure 3, the lower bound on the number of active S-boxes increases by three per round beginning with the twelfth round. Additionally, the designers supplied a 22-round linear characteristic (refer to Table 6 of [2]) with a correlation of 2^{-64}. The 22-round linear characteristic activates precisely three S-boxes in the initial 21 rounds, and its construction relies on a one-round *iterative* linear characteristic, which implies linear characteristics with identical input and output masks.

Table 3. LAT of the S-box of BAKSHEESH.

α \ β	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	-4	0	0	0	0	-4	0	-4	0	0	0
2	0	0	0	4	0	0	-4	0	0	0	4	0	0	0	0	4
3	0	0	0	0	0	-4	-4	0	0	0	0	0	4	0	0	-4
4	0	0	0	0	0	0	0	0	0	4	-4	0	4	0	0	4
5	0	0	0	-4	0	-4	0	0	0	-4	0	0	0	0	0	4
6	0	0	0	4	0	0	4	0	0	-4	0	0	4	0	0	0
7	0	0	0	0	0	4	-4	0	0	-4	-4	0	0	0	0	0
8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0
9	0	0	-4	0	4	0	0	0	0	0	0	-4	0	-4	0	0
a	0	-4	0	0	4	0	0	0	4	0	0	0	0	4	0	0
b	0	-4	-4	0	0	0	0	0	-4	0	0	4	0	0	0	0
c	0	0	0	0	0	0	0	0	4	0	0	4	0	-4	4	0
d	0	0	-4	0	-4	0	0	0	4	0	0	0	0	0	-4	0
e	0	4	0	0	4	0	0	0	0	0	0	4	0	0	-4	0
f	0	-4	4	0	0	0	0	0	0	0	0	0	0	-4	-4	0

In order to verify whether the property that the minimum number of active S-boxes increases by three per round for linear characteristics that span more than 22 rounds can be maintained, we employ the automatic tool proposed in [16] to determine the lower bound on the number of active S-boxes from 23 rounds to 35 rounds. The test result, as illustrated in Figure 3, suggests that

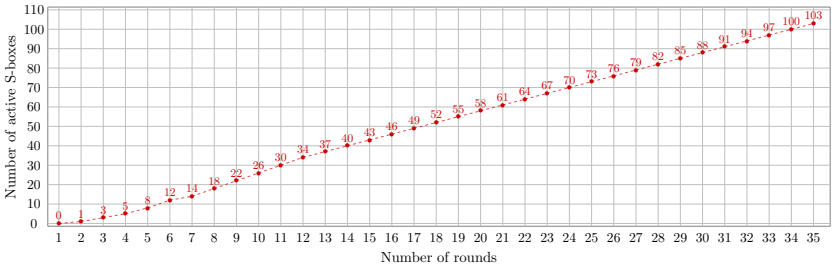


Fig. 3. Lower bound on the number of linear active S-boxes.

BAKSHEESH's R-round linear characteristics have a minimum of $(3R-2)$ active S-boxes for all $R \geqslant 12$.

These observations enhance our motivation to investigate the linear characteristics of BAKSHEESH, which spans over twelve rounds and contains three active S-boxes per round. We are interested in determining whether any additional linear characteristics activate three S-boxes per round in addition to the iterative linear characteristic described in [2]. Is it possible to enumerate all linear characteristics of BAKSHEESH that encompass more than twelve rounds and have three active S-boxes per round? The nibble-oriented description for BAKSHEESH in Section 2.3 will be employed to resolve these issues.

Note that the S-box of BAKSHEESH contains a particular linear approximation $(8, 7)$ with an absolute correlation of 1, beyond the trivial approximation $(0, 0)$. Directly examining linear characteristics with three active S-boxes per round will lead to discussing exceptional cases in which linear characteristics include $(8, 7)$ as linear approximations for specific S-boxes. As a result, the subsequent section will concentrate on linear characteristics that contain three nonzero nibbles in the input mask of each round, which encompasses the particular circumstance.

4 Positions of Nonzero Nibbles in Linear Masks

Given that the target is linear characteristics of BAKSHEESH with three nonzero nibbles in the input mask of each round, the initial question is to ascertain the positions of these nonzero nibbles. Based on the columns of three nonzero nibbles in the input mask, the issue can be divided into three cases under the nibble-oriented description of the round function.

1. All three nonzero nibbles are located in the same column of the matrix state.
2. The three nonzero nibbles are located in three distinct columns.
3. Two nonzero nibbles are located in the same column of the matrix state, while the remaining nonzero nibble is located in a different column.

In this section, we will prove that the initial two cases are unfeasible and obtain preliminary information regarding the three nonzero nibbles of the input masks of individual rounds.

4.1 Nonzero Nibbles are not Located in the Same Column

For an R-round linear characteristic with three nonzero nibbles in the input mask of each round, we assume that the three nonzero nibbles in the r-th round are situated in the same column, where $0 \leqslant r < R-1$. The column is presumed to be the first column without loss of generality. The linear approximation of the bit permutation P_{16} in the r-th round operating on the first column is denoted as $(\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3, \beta'_0\|\beta'_1\|\beta'_2\|\beta'_3)$, where three nibbles in $\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3$ are nonzero. We will prove the necessary conditions for this linear approximation to guarantee that the corresponding linear characteristic can preserve three nonzero nibbles in the input masks of the $(r-1)$-th, $(r+1)$-th, and $(r+2)$-th rounds.

Condition 1. *The output mask $\beta'_0\|\beta'_1\|\beta'_2\|\beta'_3$ of P_{16} has three nonzero nibbles.*

Proof. As shown in Figure 4, the round function ensures that $\beta'_0\|\beta'_1\|\beta'_2\|\beta'_3$ is part of the input mask for the $(r+1)$-th round. Three nibbles in $\beta'_0\|\beta'_1\|\beta'_2\|\beta'_3$ should be nonzero, as we presume that the linear characteristic has three nonzero nibbles in the input mask of each round. □

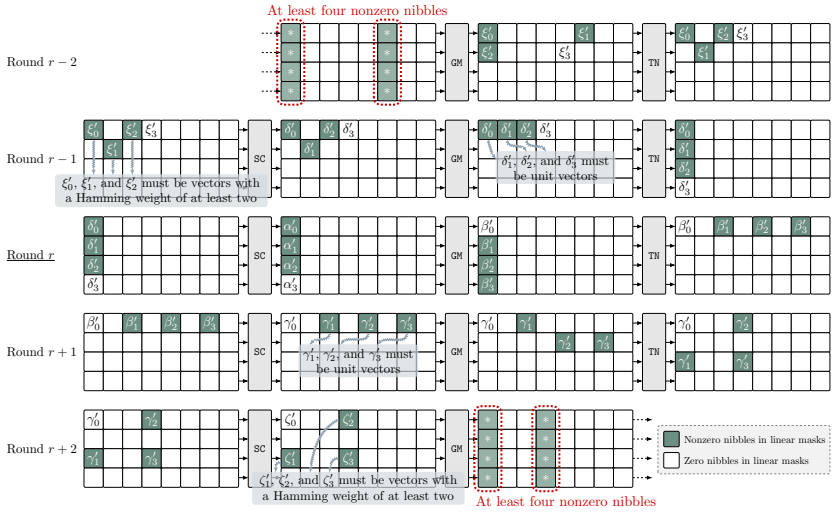


Fig. 4. Contradictions arise when three nonzero nibbles are present in the same column.

Condition 2. *When the three nonzero nibbles in $\beta'_0\|\beta'_1\|\beta'_2\|\beta'_3$ are used as input masks of S-boxes in the $(r+1)$-th round, the corresponding output masks of S-boxes should be unit vectors.*

Proof. As illustrated in Figure 4, the input masks of four S-boxes in the $(r+1)$-th round are β'_0, β'_1, β'_2, and β'_3, while the corresponding output masks are denoted as γ'_0, γ'_1, γ'_2, and γ'_3. Assume the three nonzero nibbles are β'_1, β'_2, and β'_3,

without losing generality. As per Property 1, γ'_1, γ'_2, and γ'_3 must be unit vectors to maintain three nonzero nibbles in the input mask of the $(r+2)$-th round. □

Condition 3. *When the three nonzero nibbles in $\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3$ serve as output masks of S-boxes in the r-th round, the related input masks should be unit vectors.*

Proof. Let $\delta'_0\|\delta'_1\|\delta'_2\|\delta'_3$ be the input mask of the r-th `SC` operation that corresponds to the output mask $\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3$. Assume that the three nonzero nibbles in $\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3$ are α'_0, α'_1, and α'_2, without loss of generality. As seen in Figure 4, δ'_0, δ'_1, and δ'_2 are in three distinct columns at the output of the `GM` operation in the $(r-1)$-th round. Property 1 implies that δ'_0, δ'_1, and δ'_2 must be unit vectors. □

According to Conditions 1 - 3, there are potential candidates for the linear approximation $(\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3, \beta'_0\|\beta'_1\|\beta'_2\|\beta'_3)$. By employing these candidates, the R-round linear characteristic can preserve three nonzero nibbles in the input masks of the $(r-1)$-th, $(r+1)$-th, and $(r+2)$-th rounds. Nevertheless, the situation differs when we look at the $(r-2)$-th and the $(r+3)$-th rounds.

Following the analysis in Condition 2, the three unit vectors γ'_1, γ'_2, and γ'_3 in $\gamma'_0\|\gamma'_1\|\gamma'_2\|\gamma'_3$ are located in three distinct columns at the output of the `GM` operation in the $(r+1)$-th round. γ'_1, γ'_2, and γ'_3 cannot be situated in the first four columns or the last four columns simultaneously, as demonstrated in Figure 4. Using Property 3, we can deduce that the three unit vectors γ'_1, γ'_2, and γ'_3 cannot be positioned in the same column after the `TN` operation. In the $(r+2)$-th round, $\gamma'_0\|\gamma'_1\|\gamma'_2\|\gamma'_3$ will serve as input masks for four S-boxes, and the corresponding output masks are denoted as $\zeta'_0\|\zeta'_1\|\zeta'_2\|\zeta'_3$. Table 3 shows that ζ'_1, ζ'_2, and ζ'_3 must be vectors with a Hamming weight of at least two. Based on Property 1, the minimal number of nonzero nibbles following the `GM` operation in the $(r+2)$-th round is four. This fact suggests that the input mask of the $(r+3)$-th round must contain a minimum of four nonzero nibbles. Similarly, we can demonstrate that the minimal number of nonzero nibbles in the input mask of the $(r-2)$-th round is at least four. Putting all of these findings together, we get the following proposition.

Proposition 1. *For an R-round ($R \geqslant 12$) linear characteristic of `BAKSHEESH` with three nonzero nibbles in the input mask of each round, three nonzero nibbles of the r-th round cannot be found in the same column of the matrix state for all $0 \leqslant r < R-1$.*

4.2 Nonzero Nibbles are not Located in Three Columns

Now, we discuss whether the three nonzero nibbles can be positioned in three distinct columns. For the R-round linear characteristic, the three nonzero nibbles in the r-th round's input mask, denoted as α''_0, α''_1, and α''_2, are presumed to be located in three distinct columns, where $0 \leqslant r < R-1$.

In Figure 5, we exhibit the scenario where α''_0, α''_1, and α''_2 are situated in the first, second, and fourth columns of the matrix state, respectively, without

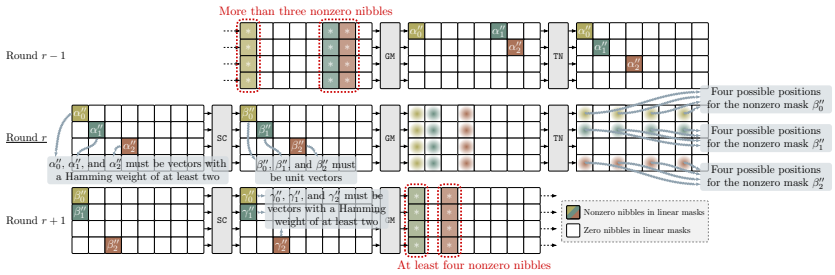


Fig. 5. When three nonzero nibbles are present in three columns, contradictions arise.

compromising its generality. Let (α_0'', β_0''), (α_1'', β_1''), and (α_2'', β_2'') be the linear approximations of the three S-boxes in the r-th round. In order to ensure that the input mask of the $(r+1)$-th round contains three nonzero nibbles, we can infer that β_0'', β_1'', and β_2'' must be unit vectors, as per Property 1. Each of the three nonzero nibbles β_0'', β_1'', and β_2'' has four potential positions in the matrix state after the $\texttt{TN} \circ \texttt{GM}$ operation. β_0'', β_1'', and β_2'' must be present in at least two columns of the input mask of the $(r+1)$-th round, as indicated by Proposition 1. Let γ_0'', γ_1'', and γ_2'' be the output masks of the $(r+1)$-th SC operation corresponding to the input masks β_0'', β_1'', and β_2''. It is evident from Table 3 that γ_0'', γ_1'', and γ_2'' must be vectors with a Hamming weight of at least two. Subsequently, Property 1 suggests that the input mask of the $(r+2)$-th round contains a minimum of four nonzero nibbles. Contradictions in the input mask of the $(r-1)$-th round can be derived using an analogous approach. By summarising the analysis above, we derive the following proposition.

Proposition 2. *Given an R-round ($R \geqslant 12$) linear characteristic of* BAKSHEESH *with three nonzero nibbles in the input mask of each round, the r-th round's three nonzero nibbles cannot be present in three distinct columns of the matrix state for all $0 \leqslant r < R-1$.*

The following proposition is reached because of the existence of BAKSHEESH's long linear characteristics, which include three nonzero nibbles in each round's input mask and the conclusions drawn from Propositions 1 and 2.

Proposition 3. *For an R-round ($R \geqslant 12$) linear characteristic of* BAKSHEESH *with three nonzero nibbles in the input mask per round, in the input mask of each round, two nonzero nibbles are always positioned in the same column of the matrix state, and the last nonzero nibble is located in a different column.*

5 Extensive Description of the Three Nonzero Nibbles

For all R-round linear characteristics of BAKSHEESH with three nonzero nibbles in the input mask of each round, preliminary information regarding the three nonzero nibbles of the input masks of individual rounds is obtained following

the analysis in Section 4. This section aims to elucidate the precise positions, concrete values, and other details of the three nonzero nibbles.

The discussion commences with the linear approximation in the r-th round, where $0 \leqslant r < R-1$ and $R \geqslant 12$. We will denote $(\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}, \beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}})$ as the linear approximation of the r-th GM operation on the column with *two* nonzero nibbles in the input mask. The linear approximation of the r-th GM operation on the column with *one* nonzero nibble in the input mask is denoted as $(\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}, \beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}})$.

5.1 Conditions for Linear Approximations on Two Columns

The initial step is establishing some essential conditions for the two linear approximations, enabling us to determine candidates for these approximations.

Condition 4. *Each nonzero nibble in* $\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}\|\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ *has a Hamming weight that is strictly less than three. The number of nonzero nibbles in* $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$ *must be three. The value of each nibble in* $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$ *should be distinct from* 8.

Proof. As illustrated in Figure 6(a), the input mask for the $(r+1)$-th round will include $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$. To guarantee that the input mask of the $(r+1)$-th round contains three nonzero nibbles, the number of nonzero nibbles in $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$ must be three. If any of the three nonzero nibbles in $\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}\|\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ has a Hamming weight greater than two, Property 1 specifies that a minimum of four nonzero nibbles will be present in $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$. This results in a contradiction. Furthermore, the output mask of one S-box in the $(r+1)$-th round must be 7 if any nibble in $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$ equals 8. It will lead to greater than three nonzero nibbles in the input mask of the $(r+2)$-th round, which is in direct opposition to our requirement for the linear characteristic. □

Condition 5. *If* $\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}$ *is in the i-th column of the matrix state, then* $\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ *must be in the* $[4 \cdot \lfloor i/4 \rfloor + (i+2) \bmod 4]$*-th column.*

Proof. Assume that the first column of the matrix state, $i = 0$, maintains the linear mask $\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}$, without loss of generality. As shown in Figure 6(b), the four nibbles $\beta_0^{\textbf{2}}$, $\beta_1^{\textbf{2}}$, $\beta_2^{\textbf{2}}$, and $\beta_3^{\textbf{2}}$ are in four different columns at the end of the r-th round because of the mapping rule of the TN∘GM operation. At the input of the TN operation, if $\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$ is in the last four columns, then all three nonzero nibbles in $\beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}}\|\beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}}$ must be in three different columns after the TN operation, which goes against Proposition 3. Through an analogous analysis of the three nonzero nibbles in the masks of the $(r-1)$-th round, it is possible to deduce that, at the input of the r-th GM operation, $\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ is not present in the first, third, fifth, and seventh columns. Summarising the analysis in the two consecutive rounds, we can conclude that $\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ can only be found in the second column. The conclusion that $\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ must be in the $[4 \cdot \lfloor i/4 \rfloor + (i+2) \bmod 4]$-th column when $\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}$ is in the i-th column is reached after analysing the cases for all $0 \leqslant i \leqslant 7$. □

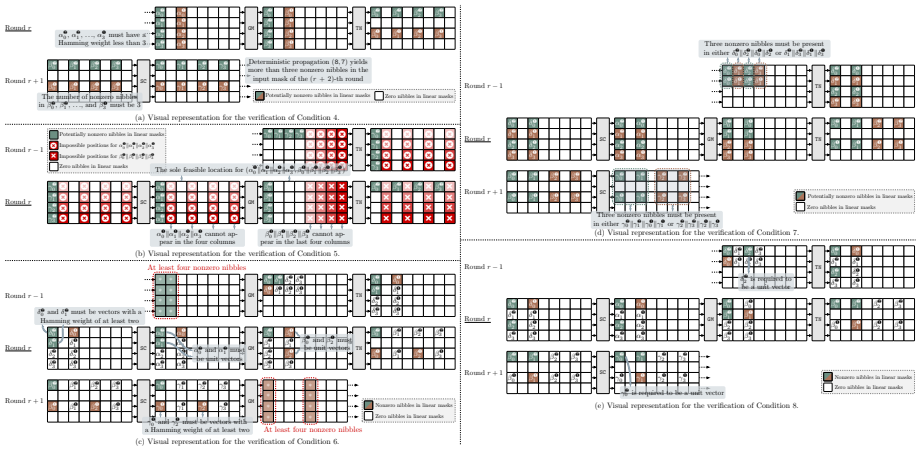


Fig. 6. Visual representation for the verification of Conditions 4 - 8.

The subsequent condition implies that the quantities of nonzero nibbles in the two columns $\beta_0^{\mathbf{2}}\|\beta_1^{\mathbf{2}}\|\beta_2^{\mathbf{2}}\|\beta_3^{\mathbf{2}}$ and $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ are deterministic.

Condition 6. *There must be two nonzero nibbles in* $\beta_0^{\mathbf{2}}\|\beta_1^{\mathbf{2}}\|\beta_2^{\mathbf{2}}\|\beta_3^{\mathbf{2}}$ *and only one nonzero nibble in the output mask* $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$*. The unique nonzero nibbles in* $\alpha_0^{\mathbf{1}}\|\alpha_1^{\mathbf{1}}\|\alpha_2^{\mathbf{1}}\|\alpha_3^{\mathbf{1}}$ *and* $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ *must be unit vectors and be identical in value. Additionally, both* $\alpha_0^{\mathbf{2}}\|\alpha_1^{\mathbf{2}}\|\alpha_2^{\mathbf{2}}\|\alpha_3^{\mathbf{2}}$ *and* $\beta_0^{\mathbf{2}}\|\beta_1^{\mathbf{2}}\|\beta_2^{\mathbf{2}}\|\beta_3^{\mathbf{2}}$ *contain at least one nonzero nibble that is not a unit vector.*

Proof. We use proof by contradiction. Assume that the number of nonzero nibbles in $\beta_0^{\mathbf{2}}\|\beta_1^{\mathbf{2}}\|\beta_2^{\mathbf{2}}\|\beta_3^{\mathbf{2}}$ is one and the number of nonzero nibbles in $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ is two. By employing Property 1, we can deduce that the two nonzero nibbles in the input mask $\alpha_0^{\mathbf{2}}\|\alpha_1^{\mathbf{2}}\|\alpha_2^{\mathbf{2}}\|\alpha_3^{\mathbf{2}}$ should be unit vectors, and the two nonzero nibbles in $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ should also be unit vectors. Let $\alpha_0^{\mathbf{2}}\|\alpha_1^{\mathbf{2}}\|\alpha_2^{\mathbf{2}}\|\alpha_3^{\mathbf{2}}$ and $\alpha_0^{\mathbf{1}}\|\alpha_1^{\mathbf{1}}\|\alpha_2^{\mathbf{1}}\|\alpha_3^{\mathbf{1}}$ be in the first and third columns, respectively, without loss of generality. The two nonzero nibbles in $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ will serve as input masks of two S-boxes in the $(r+1)$-th round, as illustrated in Figure 6(c). The output mask of the $(r+1)$-th SC operation, which corresponds to $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$, is denoted as $\gamma_0^{\mathbf{1}}\|\gamma_1^{\mathbf{1}}\|\gamma_2^{\mathbf{1}}\|\gamma_3^{\mathbf{1}}$. Hamming weights of the two nonzero nibbles in $\gamma_0^{\mathbf{1}}\|\gamma_1^{\mathbf{1}}\|\gamma_2^{\mathbf{1}}\|\gamma_3^{\mathbf{1}}$ must exceed one, as indicated by Table 3. Given that the four nibbles in $\gamma_0^{\mathbf{1}}\|\gamma_1^{\mathbf{1}}\|\gamma_2^{\mathbf{1}}\|\gamma_3^{\mathbf{1}}$ are in four distinct columns, the output mask of the subsequent GM operation will contain a minimum of four nonzero nibbles. Consequently, the $(r+2)$-th round's input mask will contain a minimum of four nonzero nibbles. A comparable analysis suggests that the input mask of the $(r-1)$-th round will also contain a minimum of four nonzero nibbles. This contradiction demonstrates that $\beta_0^{\mathbf{2}}\|\beta_1^{\mathbf{2}}\|\beta_2^{\mathbf{2}}\|\beta_3^{\mathbf{2}}$ must contain two nonzero nibbles, whereas $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ must contain only one nonzero nibble. Naturally, the unique nonzero nibbles in $\alpha_0^{\mathbf{1}}\|\alpha_1^{\mathbf{1}}\|\alpha_2^{\mathbf{1}}\|\alpha_3^{\mathbf{1}}$ and $\beta_0^{\mathbf{1}}\|\beta_1^{\mathbf{1}}\|\beta_2^{\mathbf{1}}\|\beta_3^{\mathbf{1}}$ must be unit vectors with the same values. Furthermore, if the two nonzero nibbles in both $\alpha_0^{\mathbf{2}}\|\alpha_1^{\mathbf{2}}\|\alpha_2^{\mathbf{2}}\|\alpha_3^{\mathbf{2}}$ and $\beta_0^{\mathbf{2}}\|\beta_1^{\mathbf{2}}\|\beta_2^{\mathbf{2}}\|\beta_3^{\mathbf{2}}$ are unit vectors, it is also easy to show that

the input masks of the $(r-1)$-th and $(r+2)$-th rounds will include more than three nonzero nibbles. □

Upon establishing the quantity of nonzero nibbles in $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$ and $\beta_0^{\textbf{❶}}\|\beta_1^{\textbf{❶}}\|\beta_2^{\textbf{❶}}\|\beta_3^{\textbf{❶}}$, the subsequent condition allows us to identify the coordinates of the nonzero nibbles in these masks.

Condition 7. *$\alpha_0^{\textbf{❷}}\|\alpha_1^{\textbf{❷}}\|\alpha_2^{\textbf{❷}}\|\alpha_3^{\textbf{❷}}$ has only two possible patterns: $*\|0\|*\|0$ or $0\|*\|0\|*$, where $*$ represents a nonzero nibble.*

- *The pattern of $\alpha_0^{\textbf{❶}}\|\alpha_1^{\textbf{❶}}\|\alpha_2^{\textbf{❶}}\|\alpha_3^{\textbf{❶}}$ is either $*\|0\|0\|0$ or $0\|0\|*\|0$ if $\alpha_0^{\textbf{❷}}\|\alpha_1^{\textbf{❷}}\|\alpha_2^{\textbf{❷}}\|\alpha_3^{\textbf{❷}}$ follows the pattern $*\|0\|*\|0$.*
- *The pattern of $\alpha_0^{\textbf{❶}}\|\alpha_1^{\textbf{❶}}\|\alpha_2^{\textbf{❶}}\|\alpha_3^{\textbf{❶}}$ is either $0\|*\|0\|0$ or $0\|0\|0\|*$ if $\alpha_0^{\textbf{❷}}\|\alpha_1^{\textbf{❷}}\|\alpha_2^{\textbf{❷}}\|\alpha_3^{\textbf{❷}}$ follows the pattern $0\|*\|0\|*$.*

The only two possible patterns of $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$ are $*\|*\|0\|0$ and $0\|0\|*\|*$.

- *The pattern of $\beta_0^{\textbf{❶}}\|\beta_1^{\textbf{❶}}\|\beta_2^{\textbf{❶}}\|\beta_3^{\textbf{❶}}$ is either $*\|0\|0\|0$ or $0\|*\|0\|0$ if $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$ follows the pattern $*\|*\|0\|0$.*
- *The pattern of $\beta_0^{\textbf{❶}}\|\beta_1^{\textbf{❶}}\|\beta_2^{\textbf{❶}}\|\beta_3^{\textbf{❶}}$ is either $0\|0\|*\|0$ or $0\|0\|0\|*$ if $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$ follows the pattern $0\|0\|*\|*$.*

Proof. Without losing generality, assume that $\alpha_0^{\textbf{❷}}\|\alpha_1^{\textbf{❷}}\|\alpha_2^{\textbf{❷}}\|\alpha_3^{\textbf{❷}}$ is situated in the first column of the matrix state, and $\alpha_0^{\textbf{❶}}\|\alpha_1^{\textbf{❶}}\|\alpha_2^{\textbf{❶}}\|\alpha_3^{\textbf{❶}}$ is in the third column. Figure 6(d) exhibits that the eight nibbles in $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}\|\beta_0^{\textbf{❶}}\|\beta_1^{\textbf{❶}}\|\beta_2^{\textbf{❶}}\|\beta_3^{\textbf{❶}}$ are located in four columns at the output of the r-th round. Nevertheless, the linear mask should still satisfy Condition 5 in the $(r+1)$-th round. Consequently, we have either $\beta_0^{\textbf{❷}} = \beta_1^{\textbf{❷}} = \beta_0^{\textbf{❶}} = \beta_1^{\textbf{❶}} = 0$ or $\beta_2^{\textbf{❷}} = \beta_3^{\textbf{❷}} = \beta_2^{\textbf{❶}} = \beta_3^{\textbf{❶}} = 0$.

- When $\beta_0^{\textbf{❷}} = \beta_1^{\textbf{❷}} = \beta_0^{\textbf{❶}} = \beta_1^{\textbf{❶}} = 0$, $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$ follows the pattern $0\|0\|*\|*$, and the pattern of $\beta_0^{\textbf{❶}}\|\beta_1^{\textbf{❶}}\|\beta_2^{\textbf{❶}}\|\beta_3^{\textbf{❶}}$ is either $0\|0\|*\|0$ or $0\|0\|0\|*$.
- When $\beta_2^{\textbf{❷}} = \beta_3^{\textbf{❷}} = \beta_2^{\textbf{❶}} = \beta_3^{\textbf{❶}} = 0$, $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$ follows the pattern $*\|*\|0\|0$, and the pattern of $\beta_0^{\textbf{❶}}\|\beta_1^{\textbf{❶}}\|\beta_2^{\textbf{❶}}\|\beta_3^{\textbf{❶}}$ is either $*\|0\|0\|0$ or $0\|*\|0\|0$.

Analysing the backward propagations of linear masks in the $(r-1)$-th round can yield the result about the patterns of $\alpha_0^{\textbf{❷}}\|\alpha_1^{\textbf{❷}}\|\alpha_2^{\textbf{❷}}\|\alpha_3^{\textbf{❷}}$ and $\alpha_0^{\textbf{❶}}\|\alpha_1^{\textbf{❶}}\|\alpha_2^{\textbf{❶}}\|\alpha_3^{\textbf{❶}}$. □

Condition 8. *Denote $\alpha_i^{\textbf{❷}}$ and $\alpha_j^{\textbf{❷}}$ as the two nonzero nibbles in $\alpha_0^{\textbf{❷}}\|\alpha_1^{\textbf{❷}}\|\alpha_2^{\textbf{❷}}\|\alpha_3^{\textbf{❷}}$, and $\beta_k^{\textbf{❷}}$ and $\beta_l^{\textbf{❷}}$ as the two nonzero nibbles in $\beta_0^{\textbf{❷}}\|\beta_1^{\textbf{❷}}\|\beta_2^{\textbf{❷}}\|\beta_3^{\textbf{❷}}$, where $i,j,k,l \in \{0,1,2,3\}$ with $i \neq j$ and $k \neq l$. Let $\mathbb{S}_i^{-1}$ and $\mathbb{S}_j^{-1}$ denote the sets of input masks that can propagate to $\alpha_i^{\textbf{❷}}$ and $\alpha_j^{\textbf{❷}}$, respectively. $\mathbb{S}_k$ and $\mathbb{S}_l$ denote the sets of output masks that can propagate from $\beta_k^{\textbf{❷}}$ and $\beta_l^{\textbf{❷}}$, respectively. That is,*

$$\begin{aligned}
\mathbb{S}_i^{-1} &= \{\delta_i^{\textbf{❷}} \mid (\delta_i^{\textbf{❷}}, \alpha_i^{\textbf{❷}}) \text{ is a possible linear approximation for the S-box}\},\\
\mathbb{S}_j^{-1} &= \{\delta_j^{\textbf{❷}} \mid (\delta_j^{\textbf{❷}}, \alpha_j^{\textbf{❷}}) \text{ is a possible linear approximation for the S-box}\},\\
\mathbb{S}_k &= \{\gamma_k^{\textbf{❷}} \mid (\beta_k^{\textbf{❷}}, \gamma_k^{\textbf{❷}}) \text{ is a possible linear approximation for the S-box}\},\\
\mathbb{S}_l &= \{\gamma_l^{\textbf{❷}} \mid (\beta_l^{\textbf{❷}}, \gamma_l^{\textbf{❷}}) \text{ is a possible linear approximation for the S-box}\}.
\end{aligned}$$

Then, both $\mathbb{S}_i^{-1} \cup \mathbb{S}_j^{-1}$ and $\mathbb{S}_k \cup \mathbb{S}_l$ must include at least one unit vector.

Proof. Let $\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}$ be located in the first column of the matrix state, and $\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}$ be located in the third column. By Condition 7, we presume that $i = 0$, $j = 2$, $k = 0$, $l = 1$, $\alpha_0^{\textbf{1}} \neq 0$, and $\beta_1^{\textbf{1}} \neq 0$ without compromising generality. With the propagation of the linear mask, the three nonzero nibbles in the input mask of the $(r+1)$-th round are $\beta_0^{\textbf{2}}$, $\beta_1^{\textbf{2}}$, and $\beta_1^{\textbf{1}}$, as illustrated in Figure 6(e). The output masks of the three S-boxes corresponding to $\beta_0^{\textbf{2}}$, $\beta_1^{\textbf{2}}$, and $\beta_1^{\textbf{1}}$ are denoted as $\gamma_0^{\textbf{2}}$, $\gamma_1^{\textbf{2}}$, and $\gamma_1^{\textbf{1}}$, respectively. According to Condition 6, $\gamma_0^{\textbf{2}}$ should be a unit vector, equivalent to saying that the set $\mathbb{S}_k \cup \mathbb{S}_l$ should contain at least one unit vector in the general case. By examining the backward propagations of linear masks in the $(r-1)$-th round, it is possible to determine that the union set $\mathbb{S}_i^{-1} \cup \mathbb{S}_j^{-1}$ should contain at least one unit vector. □

Conditions 4 - 8 impose constraints on linear approximations $(\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}, \beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}})$ and $(\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}, \beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}})$. Using these conditions, we can identify potential candidates for $(\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}, \beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}})$ and $(\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}, \beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}})$. The remainder of this section will explain how to evaluate these candidates further.

5.2 Further Evaluations of Candidate Linear Approximations

All candidates for the linear approximation $(\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}, \beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}})$ can be identified using Conditions 4 - 8. Following the implementation of a test, we discover that 12 candidates simultaneously validate Conditions 4 - 8. As listed in Table 4, the input and output masks of the first eight candidates C00 - C07 contain one nibble, a unit vector, and the other nibble, a vector with a Hamming weight of two. For the remaining four candidates, C08 - C11, both nonzero nibbles in the input and output masks are vectors with a Hamming weight of two. The following investigation suggests that the candidate list can be reduced gradually.

Table 4. Candidates for $(\alpha_0^{\textbf{2}}\|\alpha_1^{\textbf{2}}\|\alpha_2^{\textbf{2}}\|\alpha_3^{\textbf{2}}, \beta_0^{\textbf{2}}\|\beta_1^{\textbf{2}}\|\beta_2^{\textbf{2}}\|\beta_3^{\textbf{2}})$.

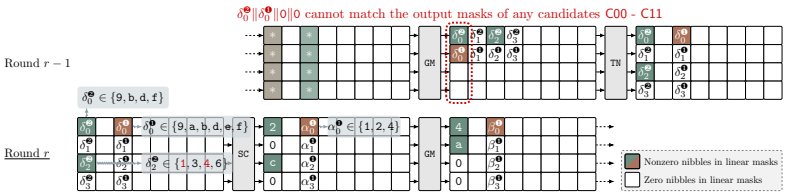
Index	Linear mask	Index	Linear mask	Index	Linear mask	Index	Linear mask
C00	(20c0, 4a00)	C01	(8030, 001a)	C02	(0209, a100)	C03	(0806, 00a4)
C04	(3080, 1a00)	C05	(c020, 004a)	C06	(0608, a400)	C07	(0902, 00a1)
C08	(30c0, 5a00)	C09	(c030, 005a)	C10	(0609, a500)	C11	(0906, 00a5)

Exclusion of C00 - C07 from the candidate list. Even though candidates C00 - C11 satisfy all the criteria outlined in Section 5.1, their ability to generate longer linear characteristics of BAKSHEESH with three nonzero nibbles in the input mask of each round is contingent upon their interaction with the other linear approximation $(\alpha_0^{\textbf{1}}\|\alpha_1^{\textbf{1}}\|\alpha_2^{\textbf{1}}\|\alpha_3^{\textbf{1}}, \beta_0^{\textbf{1}}\|\beta_1^{\textbf{1}}\|\beta_2^{\textbf{1}}\|\beta_3^{\textbf{1}})$. Additional analyses indicate that the initial eight linear approximations (C00 - C07) can be eliminated from the candidate list.

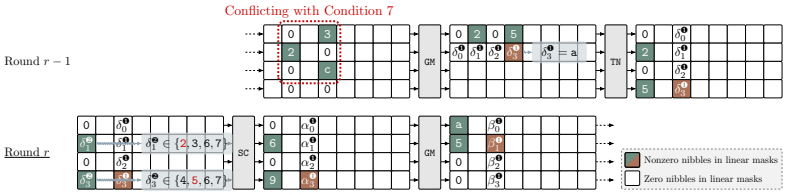
We employ the exclusion of candidate C00 as an example. As exhibited in Figure 7(a), we presume that the candidate linear approximation (20c0, 4a00) is located in the first column at the input of the r-th GM operation, without any loss of generality. The linear approximation of the third column with only one nonzero nibble is denoted as $(\alpha_0^{\blacksquare}\|\alpha_1^{\blacksquare}\|\alpha_2^{\blacksquare}\|\alpha_3^{\blacksquare}, \beta_0^{\blacksquare}\|\beta_1^{\blacksquare}\|\beta_2^{\blacksquare}\|\beta_3^{\blacksquare})$. Denote $\delta_0^{\blacksquare}$ as the input mask of the S-box that corresponds to the output mask 2, and $\delta_2^{\blacksquare}$ as the input mask of the S-box that corresponds to the output mask c. The input mask of the SC operation corresponding to $\alpha_0^{\blacksquare}\|\alpha_1^{\blacksquare}\|\alpha_2^{\blacksquare}\|\alpha_3^{\blacksquare}$ is denoted as $\delta_0^{\blacksquare}\|\delta_1^{\blacksquare}\|\delta_2^{\blacksquare}\|\delta_3^{\blacksquare}$. Table 3 yields $\delta_0^{\blacksquare} \in \{9, b, d, f\}$ and $\delta_2^{\blacksquare} \in \{1, 3, 4, 6\}$. That is, it is impossible for $\delta_0^{\blacksquare}$ to be a unit vector. Then, $\delta_0^{\blacksquare}$ and $\delta_2^{\blacksquare}$ will be situated in two distinct columns at the output of the GM operation when the linear mask is backwards propagated to the $(r-1)$-th round. Condition 6 implies that $\delta_2^{\blacksquare}$ must be a unit vector and that $\delta_0^{\blacksquare}$ should be the sole nonzero nibble in $\delta_0^{\blacksquare}\|\delta_1^{\blacksquare}\|\delta_2^{\blacksquare}\|\delta_3^{\blacksquare}$. Consequently, $\alpha_0^{\blacksquare}$ should be assigned values from the set $\{1, 2, 4\}$, and $\delta_0^{\blacksquare}$ is a member of the set $\{9, a, b, d, e, f\}$, according to Table 3. $\delta_0^{\blacksquare}\|\delta_0^{\blacksquare}\|0\|0$ should theoretically correspond to the output mask of at least one candidate in Table 4, as it is a column that is part of the output mask of the GM operation in the $(r-1)$-th round, and it is the column with two nonzero nibbles. Nevertheless, this type of correspondence does not exist, as both $\delta_0^{\blacksquare}$ and $\delta_0^{\blacksquare}$ can only accept values greater than 8. Hence, the linear approximation (20c0, 4a00) is insufficient to generate the long linear characteristics of BAKSHEESH that we require. An analogous analysis can be conducted to eliminate the linear approximations C01 - C07 from the candidate list.

Exclusion of C10 and C11 from the candidate list. Currently, we are left with four potential linear approximations, C08 - C11. A short inspection reveals that the values of the two nonzero nibbles in the C08 - C11 output masks are deterministic: one equals 5, and the other equals a. This property enables the further elimination of candidates C10 and C11.

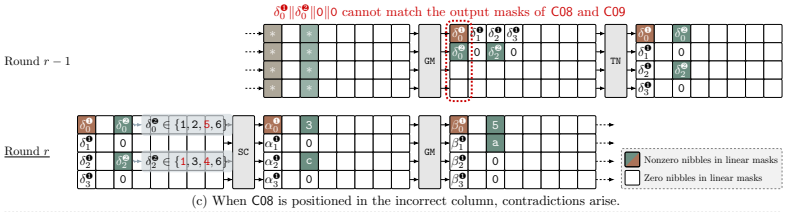
The exclusion of C10 serves as an illustration. As shown in Figure 7(b), we suppose that the candidate linear approximation (0609, a500) is situated in the first column at the input of the r-th GM operation, without any loss of generality. The input masks of the S-box that correspond to the output masks 6 and 9 are denoted as $\delta_1^{\blacksquare}$ and $\delta_3^{\blacksquare}$, respectively. We may ascertain that $\delta_1^{\blacksquare} \in \{2, 3, 6, 7\}$ and $\delta_3^{\blacksquare} \in \{4, 5, 6, 7\}$ by utilising Table 3. As a result of the previously described property and Condition 8, $\delta_1^{\blacksquare}$ and $\delta_3^{\blacksquare}$ have unique values, namely $\delta_1^{\blacksquare} = 2$ and $\delta_3^{\blacksquare} = 5$. When these masks are backwards propagated to the $(r-1)$-th round, the linear mask at the fourth column is $5\|\delta_3^{\blacksquare}\|0\|0$ at the output of the GM operation. Based on the output masks of the final four candidates in Table 4, it is evident that $\delta_3^{\blacksquare} = a$. Consequently, the input mask of the GM operation corresponding to $5\|\delta_3^{\blacksquare}\|0\|0$ can only be 30c0. Meanwhile, the second column of the input mask for the GM operation is of the form $0\|*\|0\|0$, as per the mapping rule of the permutation P_{16}. It contradicts Condition 7.



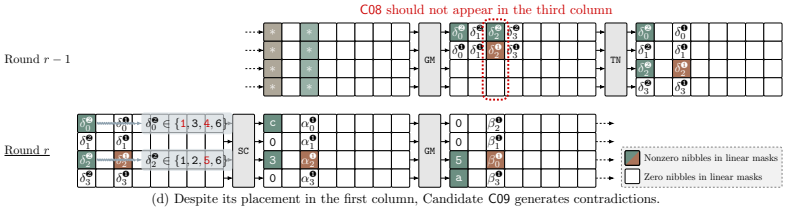
(a) Candidate C00 yields contradictions.



(b) Candidate C10 yields contradictions.



(c) When C08 is positioned in the incorrect column, contradictions arise.



(d) Despite its placement in the first column, Candidate C09 generates contradictions.

Fig. 7. Exclusion of candidates C00 - C07, C09 - C11.

Exclusion of C09 from the candidate list. So far, we have only two candidates for $(\alpha_0^{❷}\|\alpha_1^{❷}\|\alpha_2^{❷}\|\alpha_3^{❷}, \beta_0^{❷}\|\beta_1^{❷}\|\beta_2^{❷}\|\beta_3^{❷})$: $(\texttt{30c0}, \texttt{5a00})$ and $(\texttt{c030}, \texttt{005a})$. It is important to note that the input masks of the two candidates are of form $*\|\texttt{0}\|*\|\texttt{0}$, and the nonzero nibble 5 is present only in the first and third positions of the output masks. Using these properties, we first show that the linear mask $\alpha_0^{❷}\|\alpha_1^{❷}\|\alpha_2^{❷}\|\alpha_3^{❷}$ must be situated in the first column at the input of the GM operation of the r-th round.

An impossible case in which the linear approximation $(\texttt{30c0}, \texttt{5a00})$ is positioned in the third column at the input of the r-th GM operation is illustrated in Figure 7(c). Denote $\delta_0^{❷}$ and $\delta_2^{❷}$ as the input masks of the S-box that correspond to the output masks 3 and c, respectively. Table 3 indicates that $\delta_0^{❷} \in \{\texttt{1}, \texttt{2}, \texttt{5}, \texttt{6}\}$ and $\delta_2^{❷} \in \{\texttt{1}, \texttt{3}, \texttt{4}, \texttt{6}\}$. Note that $\delta_0^{❷}$ and $\delta_2^{❷}$ will contribute to the output mask of the GM operation in the $(r-1)$-th round. Because C08 and C09 are the only remaining candidates, the output mask of the $(r-1)$-th GM operation must contain either 5a00 or 005a in one column. In order to guarantee that 5 is present in the output mask of the $(r-1)$-th GM operation, $\delta_0^{❷}$ must be equal to 5. Nevertheless, the first column $\delta_0^{❶}\|\delta_0^{❷}\|\texttt{0}\|\texttt{0}$ of the output mask of the $(r-1)$-th GM operation is of form $*\|\texttt{5}\|\texttt{0}\|\texttt{0}$, which is incompatible with 5a00 or 005a in any event.

Then, a comparable approach can eliminate the case in which candidate C09 is positioned in the first column of the matrix state. Figure 7(d) serves as an illustration, in which the linear approximation $(\texttt{c030}, \texttt{005a})$ is in the first column of the GM operation during the r-th round. After the linear mask propagates back to the $(r-1)$-th round, the output mask of the GM operation at the third column must be 5a00, and the linear approximation on this column must be the candidate C08. However, as depicted in Figure 7(c), the $(r-2)$-th round will result in a contradiction when C08 is positioned in the third column. Consequently, the candidate C09 is eliminated from the candidate list.

Using the sole remaining candidate, C08, we can establish a 1-round iterative linear characteristic with three active S-boxes, as illustrated in Figure 8. Due to its uniqueness, we can infer that any R-round $(R \geqslant 12)$ linear characteristics of BAKSHEESH with three active S-boxes in each round must be constructed with this one-round linear characteristic.

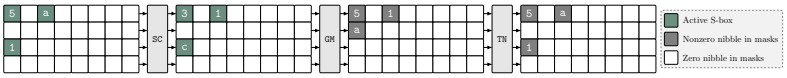


Fig. 8. One-round iterative linear characteristic with three active S-boxes.

6 All Optimal Linear Characteristics of BAKSHEESH

BAKSHEESH's R-round linear characteristics should exhibit a correlation of $2^{-3 \cdot R}$ when three S-boxes are activated per round. But the correlation of BAKSHEESH's R-round optimal linear characteristic is $2^{-3 \cdot R+2}$ for $R \geqslant 12$, as illustrated in

Figure 3. We believe the inconsistency is due to the existence of the nontrivial linear approximation $(8, 7)$ for the S-box, with an absolute correlation of 1. We can reduce the number of active S-boxes in the $(R-1)$-th round by revising the output masks of the three active S-boxes in the $(R-2)$-th round using this linear approximation. As seen in Figure 9(d), four possible propagations ensure the number of active S-boxes in the $(R-1)$-th round is one after further analysis.

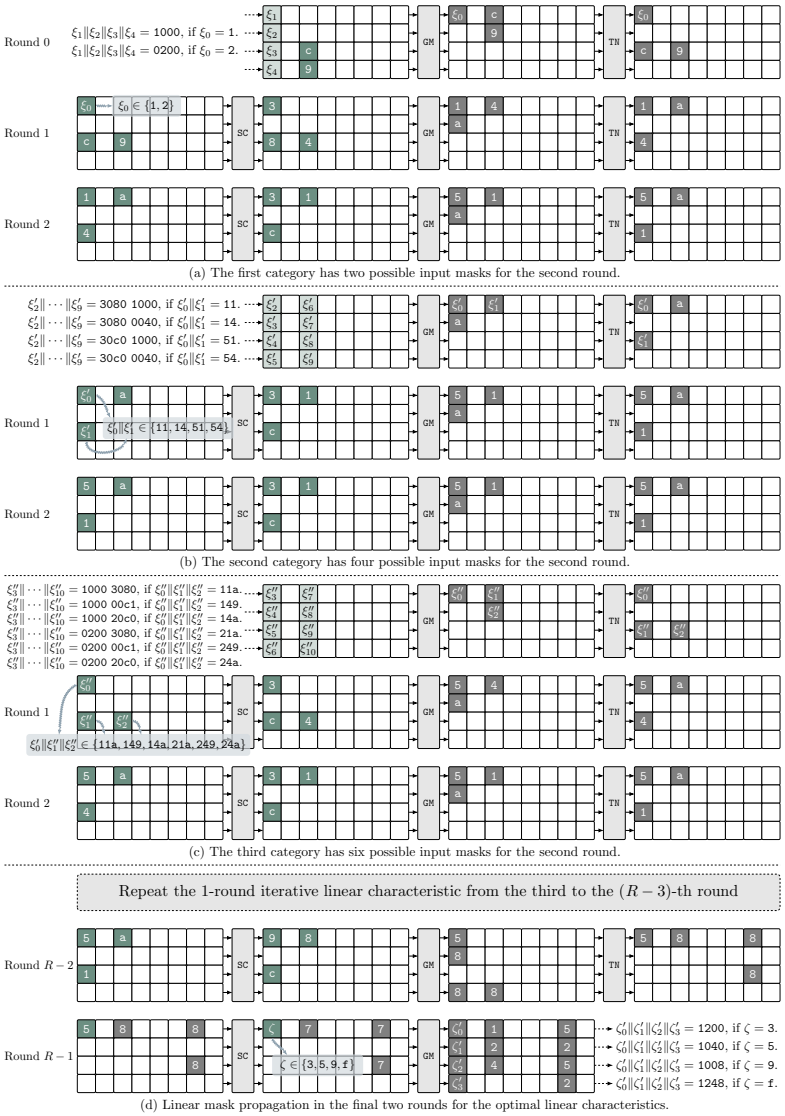
Another interesting task is determining how many R-round ($R \geqslant 12$) optimal linear characteristics of BAKSHEESH we can construct. We discover that the linear approximation in the first three rounds of the R-round optimal linear characteristics may differ from the one depicted in Figure 8 by examining the propagation of the linear mask in the first few rounds. Figure 9(a) - 9(c) demonstrates that the optimal linear characteristics can be classified into three categories based on the linear mask propagations in the second and third rounds. Two, four, and six potential linear mask propagations exist in the first, second, and third categories, respectively. Given that each of the three active S-boxes in the initial rounds has four potential input masks, the first three rounds of all the optimal R-round linear characteristics have $(2 + 4 + 6) \cdot 4^3 = 768$ possibilities. Considering the four possible propagations in the final two rounds, as illustrated in Figure 9(d), the maximum number of R-round optimal linear characteristics of BAKSHEESH that can be generated is 3072.

We employ the automatic tool introduced in [16] to find all optimal R-round linear characteristics of BAKSHEESH for all $12 \leqslant R \leqslant 35$. The test results indicate that BAKSHEESH's total number of optimal R-round linear characteristics is indeed 3072. To put it differently, the linear characteristics produced by the linear characteristics illustrated in Figure 9 are all the optimal R-round linear characteristics of BAKSHEESH when $R \geqslant 12$.

7 Conclusion

This paper presents an exhaustive analysis of the optimal linear characteristics of the lightweight block cipher BAKSHEESH. Initially, an explicit formula for the absolute correlation of BAKSHEESH's R-round optimal linear characteristic is proposed when $R \geqslant 12$. In light of all observations encouraging us to examine the linear characteristics of BAKSHEESH with three active S-boxes per round, we first derive some properties of the three active S-boxes in each round. Then, we illustrate that there is only one 1-round iterative linear characteristic with three active S-boxes. This 1-round linear characteristic must be included in any R-round ($R \geqslant 12$) linear characteristics of BAKSHEESH with three active S-boxes in each round, as it is unique. Lastly, we show that, for $R \geqslant 12$, the total number of R-round optimal linear characteristics of BAKSHEESH is 3072. All of these characteristics can be created using the 1-round iterative linear characteristic.

Acknowledgements The research leading to these results has received funding from the National Natural Science Foundation of China (Grant No. 62272273,



(a) The first category has two possible input masks for the second round.

(b) The second category has four possible input masks for the second round.

(c) The third category has six possible input masks for the second round.

(d) Linear mask propagation in the final two rounds for the optimal linear characteristics.

Fig. 9. Construction of all R-round ($R \geqslant 12$) optimal linear characteristics.

Grant No. 62002201, Grant No. 62032014), the National Key Research and Development Program of China (Grant No. 2018YFA0704702), and the Major Basic Research Project of Natural Science Foundation of Shandong Province, China (Grant No. ZR202010220025). Ling Sun gratefully acknowledges the support by the Program of TaiShan Scholars Special Fund for young scholars (Grant No. tsqn202306043).

References

1. Baksi, A., Baksi, A.: Default: Cipher-level resistance against differential fault attack. Classical and Physical Security of Symmetric Key Cryptographic Algorithms pp. 177–216 (2022)
2. Baksi, A., Breier, J., Chattopadhyay, A., Gerlich, T., Guilley, S., Gupta, N., Isobe, T., Jati, A., Jedlicka, P., Kim, H., et al.: Baksheesh: similar yet different from gift. Cryptology ePrint Archive (2023)
3. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21. pp. 411–436. Springer (2015)
4. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: Gift: A small present: Towards reaching the limit of lightweight encryption. In: Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. pp. 321–345. Springer (2017)
5. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The simon and speck lightweight block ciphers. In: Proceedings of the 52nd annual design automation conference. pp. 1–6 (2015)
6. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., 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 36. pp. 123–153. Springer (2016)
7. Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., Verbauwhede, I.: Spongent: A lightweight hash function. In: Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. pp. 312–325. Springer (2011)
8. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: Present: An ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. pp. 450–466. Springer (2007)
9. De Canniere, C., Dunkelman, O., Knežević, M.: Katan and ktantan—a family of small and efficient hardware-oriented block ciphers. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 272–288. Springer (2009)
10. Guo, J., Peyrin, T., Poschmann, A.: The photon family of lightweight hash functions. In: Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31. pp. 222–239. Springer (2011)
11. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The led block cipher. In: Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. pp. 326–341. Springer (2011)
12. Matsui, M.: Linear cryptanalysis method for des cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 386–397. Springer (1993)
13. Rijmen, V., Daemen, J.: Advanced encryption standard. Proceedings of federal information processing standards publications, national institute of standards and technology **19**, 22 (2001)

14. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: an ultra-lightweight blockcipher. In: Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. pp. 342–357. Springer (2011)
15. Sun, L., Preneel, B., Wang, W., Wang, M.: A greater gift: Strengthening gift against statistical cryptanalysis. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 115–144. Springer (2022)
16. Sun, L., Wang, W., Wang, M.: Accelerating the search of differential and linear characteristics with the sat method. IACR Transactions on Symmetric Cryptology pp. 269–315 (2021)