A Greater GIFT: Strengthening GIFT against Statistical Cryptanalysis

Ling Sun[1], Bart Preneel[2], Wei Wang[1], Meiqin Wang[1](✉)

{lingsun, weiwangsdu, mqwang}@sdu.edu.cn, bart.preneel@kuleuven.be

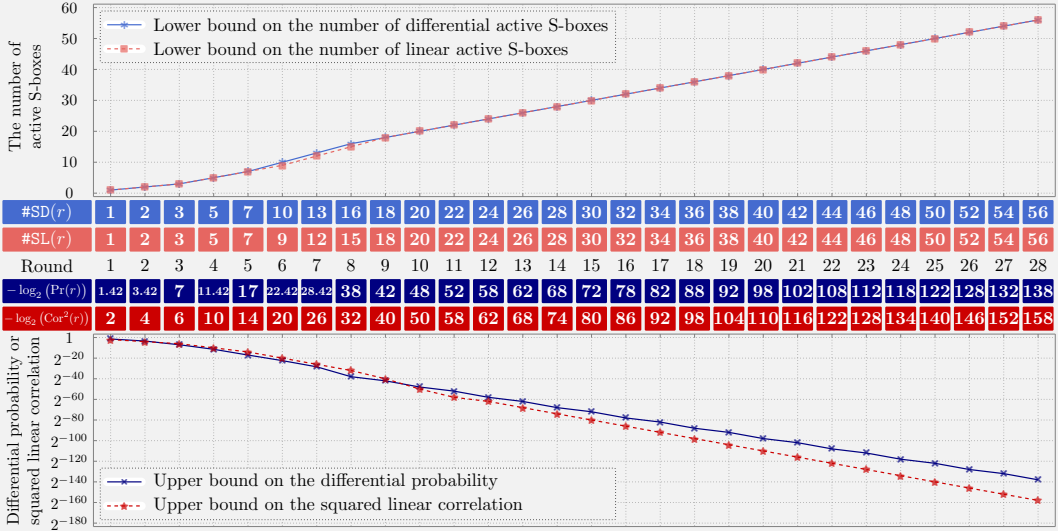
1. Shandong University, Jinan & Qingdao, China
2. Department of Electrical Engineering-ESAT, KU Leuven and imec, Leuven, Belgium

EUROCRYPT 2022 @ June, 2022

山东大学
SHANDONG UNIVERSITY

Outline

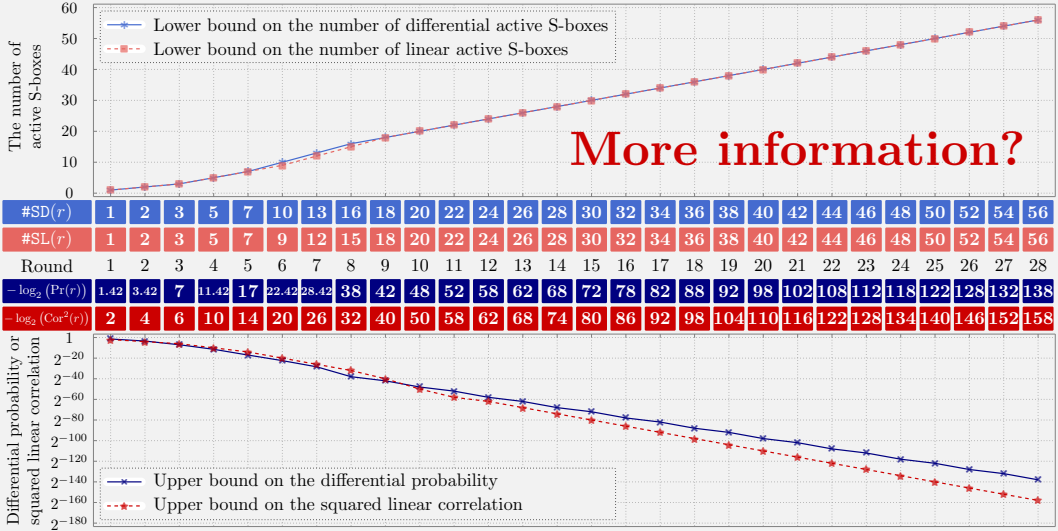
Motivation



#SD(r)	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
#SL(r)	1	2	3	5	7	9	12	15	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56

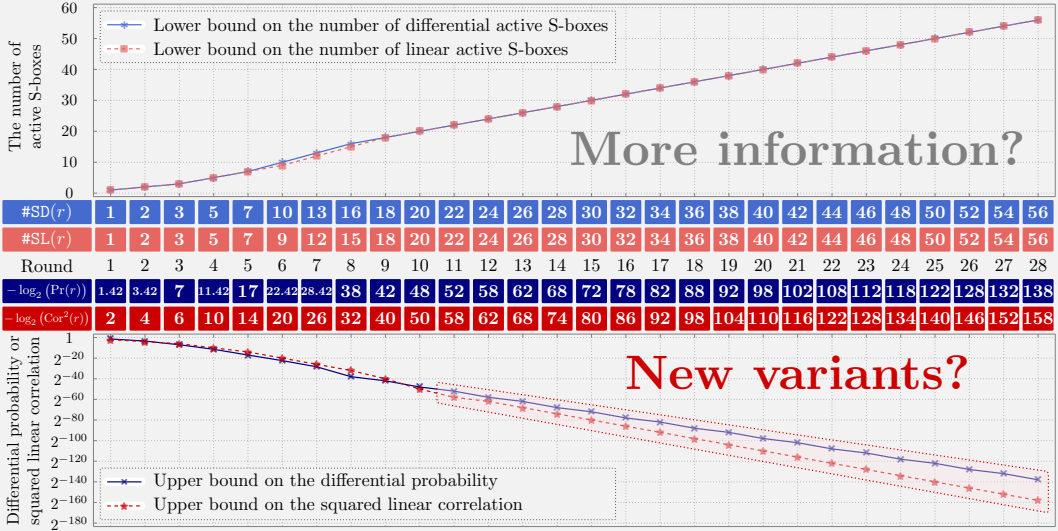
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$-\log_2(\Pr(r))$	1.42	3.42	7	11.42	17	22.42	28.42	38	42	48	52	58	62	68	72	78	82	88	92	98	102	108	112	118	122	128	132	138
$-\log_2(\mathrm{Cor}^2(r))$	2	4	6	10	14	20	26	32	40	50	58	62	68	74	80	86	92	98	104	110	116	122	128	134	140	146	152	158

Motivation



#SD(r)	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
#SL(r)	1	2	3	5	7	9	12	15	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$-\log_2(\Pr(r))$	1.42	3.42	7	11.42	17	22.42	28.42	38	42	48	52	58	62	68	72	78	82	88	92	98	102	108	112	118	122	128	132	138
$-\log_2(\mathrm{Cor}^2(r))$	2	4	6	10	14	20	26	32	40	50	58	62	68	74	80	86	92	98	104	110	116	122	128	134	140	146	152	158

Motivation



#SD(r)	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
#SL(r)	1	2	3	5	7	9	12	15	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56

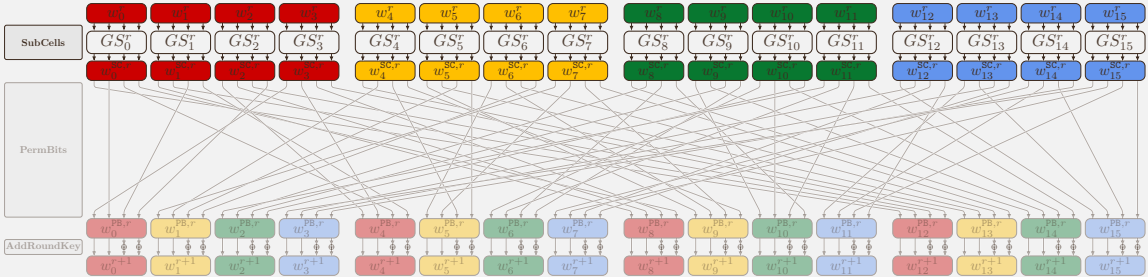
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$-\log_2(\Pr(r))$	1.42	3.42	7	11.42	17	22.42	28.42	38	42	48	52	58	62	68	72	78	82	88	92	98	102	108	112	118	122	128	132	138
$-\log_2(\mathrm{Cor}^2(r))$	2	4	6	10	14	20	26	32	40	50	58	62	68	74	80	86	92	98	104	110	116	122	128	134	140	146	152	158

Outline

- Motivation.
- **Preliminaries.**
- Differential and Linear Properties of GIFT-64.
- Can We Improve GIFT-64?
- Conclusion.

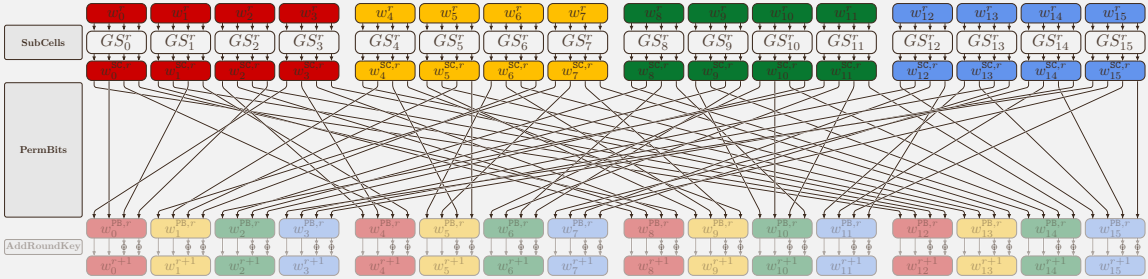
Specification of GIFT-64

- GIFT is a family of lightweight block ciphers proposed by Banik *et al.* .
- GIFT-64, a 64-bit block cipher with a 128-bit key and with 28 rounds.
- Each round consists of three steps.



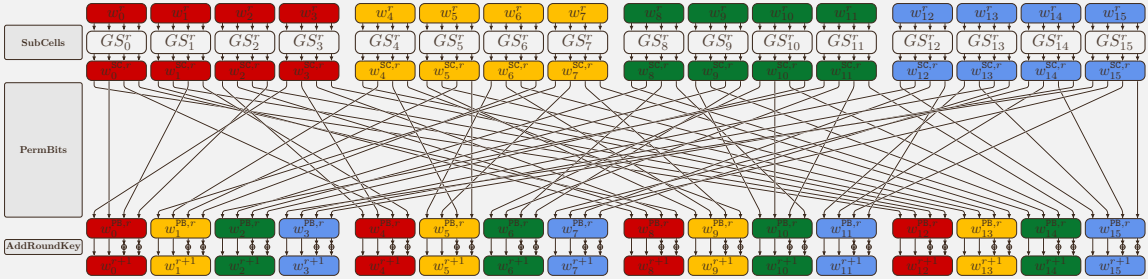
Specification of GIFT-64

- GIFT is a family of lightweight block ciphers proposed by Banik *et al.* .
- GIFT-64, a 64-bit block cipher with a 128-bit key and with 28 rounds.
- Each round consists of three steps.



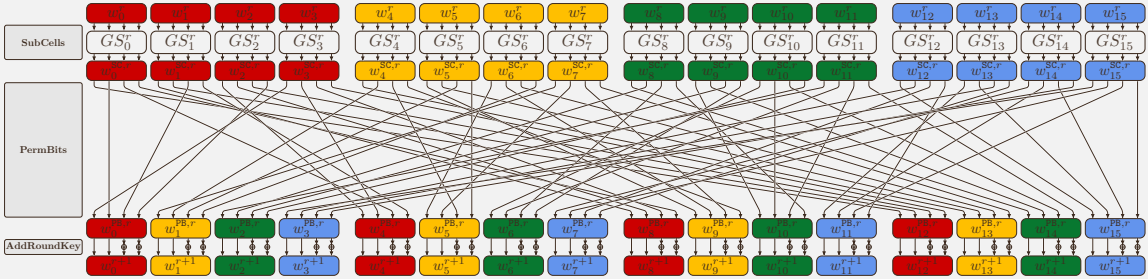
Specification of GIFT-64

- GIFT is a family of lightweight block ciphers proposed by Banik *et al.* .
- GIFT-64, a 64-bit block cipher with a 128-bit key and with 28 rounds.
- Each round consists of three steps.



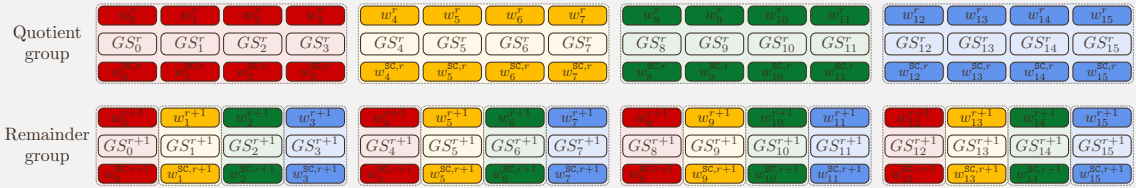
Specification of GIFT-64

- GIFT is a family of lightweight block ciphers proposed by Banik *et al.* .
- GIFT-64, a 64-bit block cipher with a 128-bit key and with 28 rounds.
- Each round consists of three steps.



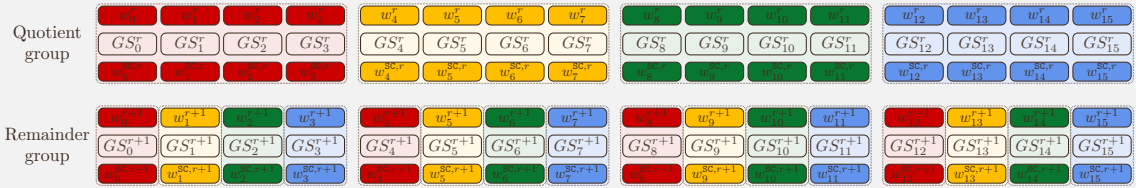
- Ten years after the publication of PRESENT (Bogdanov *et al.* @ CHES 2007).
- Much-increased efficiency in hardware and software implementations.
- Avoid consecutive 1-1 bit differential and linear transitions in the cipher.

"Bad Output must go to Good Input (BOGI)"Paradigm



- 64-bit permutation $\Rightarrow$ four independent and identical 16-bit permutations.

"Bad Output must go to Good Input (BOGI)"Paradigm

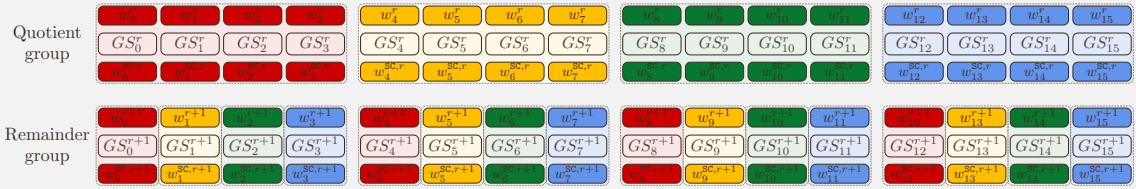


- 64-bit permutation $\Rightarrow$ four independent and identical 16-bit permutations.

Δx \ Δy	0x1	0x2	0x4	0x8
0x1	0	0	0	2
0x2	0	0	0	0
0x4	0	0	0	0
0x8	0	0	0	0

- Good input: $GI = \{0, 1, 2\}$.
- Bad input: $BI = \{3\}$.
- Good output: $GO = \{1, 2, 3\}$.
- Bad output: $BO = \{0\}$.

"Bad Output must go to Good Input (BOGI)"Paradigm



- 64-bit permutation $\Rightarrow$ four independent and identical 16-bit permutations.

Δx \ Δy	0x1	0x2	0x4	0x8
0x1	0	0	0	2
0x2	0	0	0	0
0x4	0	0	0	0
0x8	0	0	0	0

- Good input: $GI = \{0, 1, 2\}$.
- Bad input: $BI = \{3\}$.
- Good output: $GO = \{1, 2, 3\}$.
- Bad output: $BO = \{0\}$.

- Differential BOGI permutation $\pi : BO \cup GO \rightarrow BI \cup GI$ with $\pi(BO) = \{\pi(i) \mid i \in BO\} \subseteq GI$.
- BOGI permutation $\Leftarrow$ Differential BOGI permutation & Linear BOGI permutation.
- For GIFT, the BOGI permutation is fixed as the identity mapping $\pi(i) = i$.

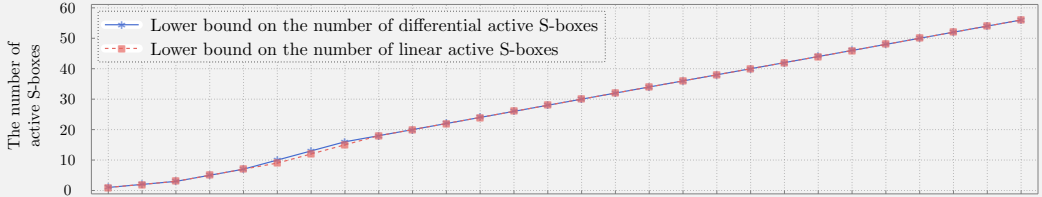
Outline

- Motivation.
- Preliminaries.
- **Differential and Linear Properties of GIFT-64.**
- Can We Improve GIFT-64?
- Conclusion.

Optimal Differential Characteristic of GIFT-64

Observations on experimental results

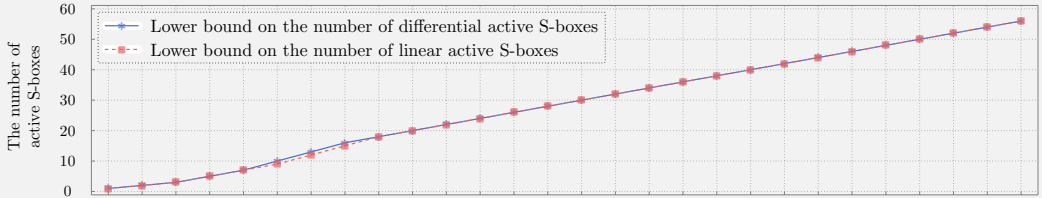
1. The minimum number of differential active S-boxes $\#\mathrm{SD}(r)$ is linearly dependent on r for all $r \geqslant 8$.
2. The optimal characteristics for more than seven rounds always activate two S-boxes in each round.



Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\#\mathrm{SD}(r)$	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
$\#\mathrm{SL}(r)$	1	2	3	5	7	9	12	15	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56

Observations on experimental results

1. The minimum number of differential active S-boxes $\#\mathrm{SD}(r)$ is linearly dependent on r for all $r \geqslant 8$.
2. The optimal characteristics for more than seven rounds always activate two S-boxes in each round.



$\#\mathrm{SD}(r)$	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
$\#\mathrm{SL}(r)$	1	2	3	5	7	9	12	15	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

- Is there a characteristic with a single active S-box in some rounds achieving the maximum differential probability?

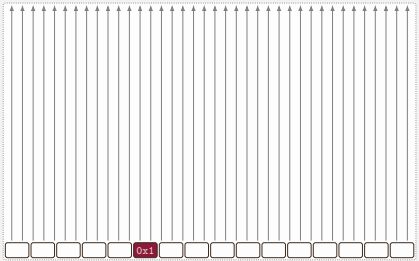
Optimal Differential Characteristic of GIFT-64

- $\mathbb{D}_{\texttt{0x1}} = \{$characteristics with at least one round having a single S-box with $\Delta_{in} = \texttt{0x1}\}$.
- Calculating a lower bound on the number of active S-boxes for characteristics in $\mathbb{D}_{\texttt{0x1}}$.

Optimal Differential Characteristic of GIFT-64

- $\mathbb{D}_{\texttt{0x1}} = \{$characteristics with at least one round having a single S-box with $\Delta_{in} = \texttt{0x1}\}$.
- Calculating a lower bound on the number of active S-boxes for characteristics in $\mathbb{D}_{\texttt{0x1}}$.

Step 1 Lower bound ($\#\mathrm{SD}^{\downarrow}_{\texttt{0x1}}(r)$) for characteristics with input differences having a single nonzero nibble 0x1.

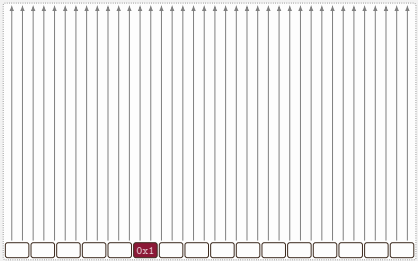


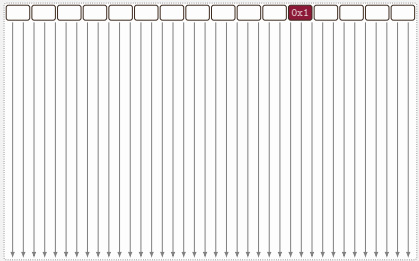
Optimal Differential Characteristic of GIFT-64

- $\mathbb{D}_{\texttt{0x1}} = \{$characteristics with at least one round having a single S-box with $\Delta_{in} = \texttt{0x1}\}$.
- Calculating a lower bound on the number of active S-boxes for characteristics in $\mathbb{D}_{\texttt{0x1}}$.

Step 1 Lower bound ($\#\mathrm{SD}^{\downarrow}_{\texttt{0x1}}(r)$) for characteristics with input differences having a single nonzero nibble 0x1.

Step 2 Lower bound ($\#\mathrm{SD}^{\uparrow}_{\texttt{0x1}}(r)$) with output differences holding a single nonzero nibble 0x1.



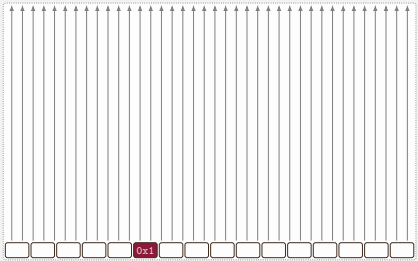


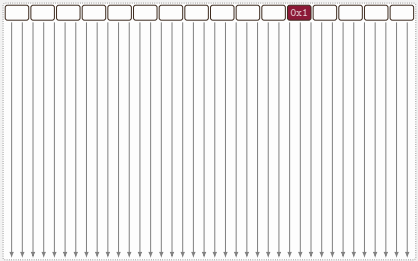
Optimal Differential Characteristic of GIFT-64

- $\mathbb{D}_{\texttt{0x1}} = \{\text{characteristics with at least one round having a single S-box with } \Delta_{in} = \texttt{0x1}\}$.
- Calculating a lower bound on the number of active S-boxes for characteristics in $\mathbb{D}_{\texttt{0x1}}$.

Step 1 Lower bound ($\#\mathrm{SD}^{\downarrow}_{\texttt{0x1}}(r)$) for characteristics with input differences having a single nonzero nibble 0x1.

Step 2 Lower bound ($\#\mathrm{SD}^{\uparrow}_{\texttt{0x1}}(r)$) with output differences holding a single nonzero nibble 0x1.



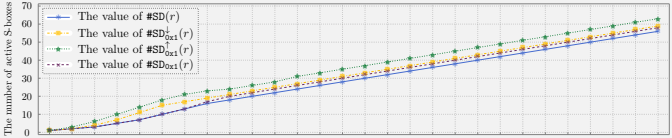


Step 3 Lower bound ($\#\mathrm{SD}_{\texttt{0x1}}(r)$) for characteristics in $\mathbb{D}_{\texttt{0x1}}$.

$$\#\mathrm{SD}_{\texttt{0x1}}(r) \geqslant \min\left\{ \#\mathrm{SD}^{\uparrow}_{\texttt{0x1}}(r_1) + \#\mathrm{SD}^{\downarrow}_{\texttt{0x1}}(r_2) \;\middle|\; r_1 + r_2 = r,\, r_1 \geqslant 0,\, r_2 \geqslant 0 \right\},$$

Optimal Differential Characteristic of GIFT-64

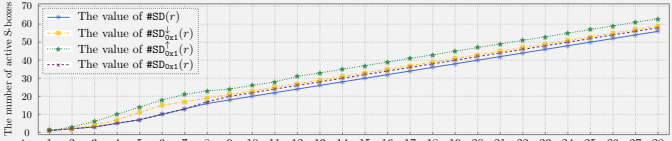
- $\#\mathrm{SD}_{0\mathtt{x}1}(r) > \#\mathrm{SD}(r)$ for all $r \geqslant 8$.
- $\#\mathrm{SD}_{\mathtt{i}}(r) > \#\mathrm{SD}(r)$ for all $r \geqslant 8$ and $\mathtt{i} \in \mathbb{F}_2^4 \setminus \{0\mathtt{x}0\}$.



Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\#\mathrm{SD}(r)$	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
$\#\mathrm{SD}^{1}_{0\mathtt{x}1}(r)$	1	2	4	7	11	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59
$\#\mathrm{SD}^{2}_{0\mathtt{x}1}(r)$	1	3	6	10	14	18	21	23	24	26	28	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
$\#\mathrm{SD}_{0\mathtt{x}1}(r)$	1	2	3	5	7	10	13	17	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58

Optimal Differential Characteristic of GIFT-64

- $\#\mathrm{SD}_{0\mathrm{x}1}(r) > \#\mathrm{SD}(r)$ for all $r \geqslant 8$.
- $\#\mathrm{SD}_{\mathtt{i}}(r) > \#\mathrm{SD}(r)$ for all $r \geqslant 8$ and $\mathtt{i} \in \mathbb{F}_2^4 \setminus \{0\mathrm{x}0\}$.



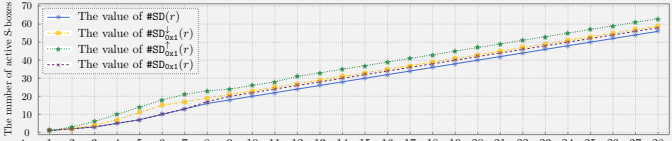
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\#\mathrm{SD}(r)$	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
$\#\mathrm{SD}^{1}_{0\mathrm{x}1}(r)$	1	2	4	7	11	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59
$\#\mathrm{SD}^{2}_{0\mathrm{x}1}(r)$	1	3	6	10	14	18	21	23	24	26	28	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
$\#\mathrm{SD}_{0\mathrm{x}1}(r)$	1	2	3	5	7	10	13	17	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58

Proposition 1

- If $r \geqslant 8$, the optimal r-round differential characteristic of GIFT-64 with the minimum number of active S-boxes must have two active S-boxes in each round.

Optimal Differential Characteristic of GIFT-64

- $\#\mathrm{SD}_{0x1}(r) > \#\mathrm{SD}(r)$ for all $r \geqslant 8$.
- $\#\mathrm{SD}_{\mathtt{i}}(r) > \#\mathrm{SD}(r)$ for all $r \geqslant 8$ and $\mathtt{i} \in \mathbb{F}_2^4 \setminus \{0x0\}$.



Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\#\mathrm{SD}(r)$	1	2	3	5	7	10	13	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
$\#\mathrm{SD}^{1}_{0x1}(r)$	1	2	4	7	11	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59
$\#\mathrm{SD}^{2}_{0x1}(r)$	1	3	6	10	14	18	21	23	24	26	28	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
$\#\mathrm{SD}_{0x1}(r)$	1	2	3	5	7	10	13	17	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58

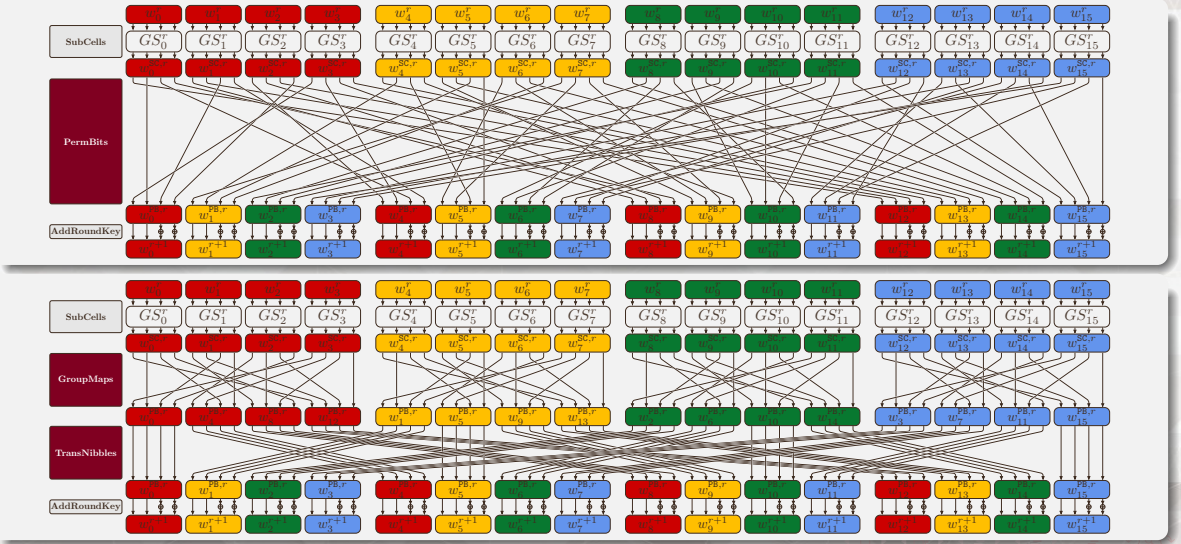
Proposition 1

- If $r \geqslant 8$, the optimal r-round differential characteristic of GIFT-64 with the minimum number of active S-boxes must have two active S-boxes in each round.

Proposition 2

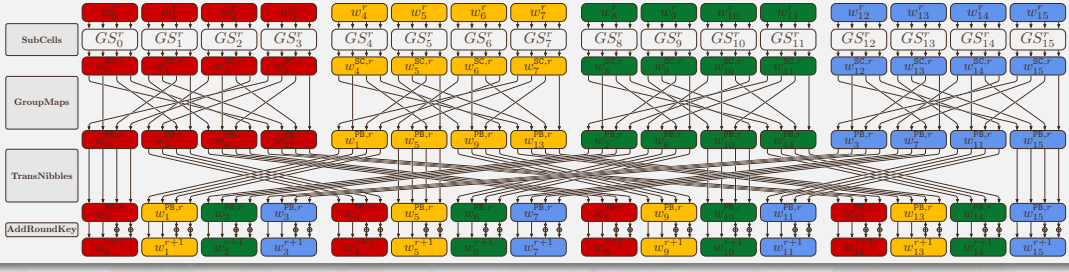
- If $r \geqslant 8$, the optimal r-round differential characteristic with the maximum probability must activate at least two S-boxes per round.

Alternative Description for the Round Function



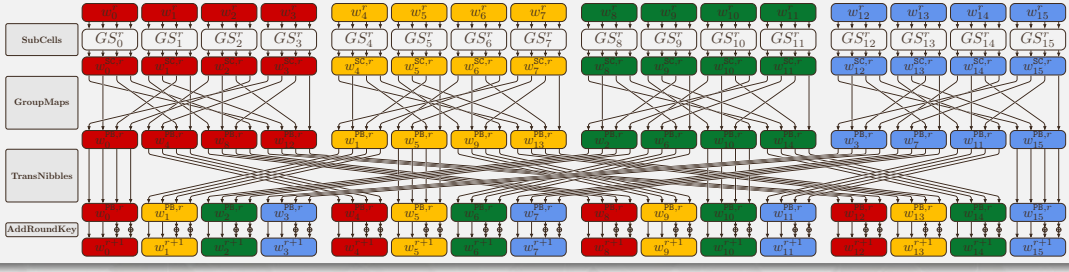
Alternative Description for the Round Function

Bit-oriented description

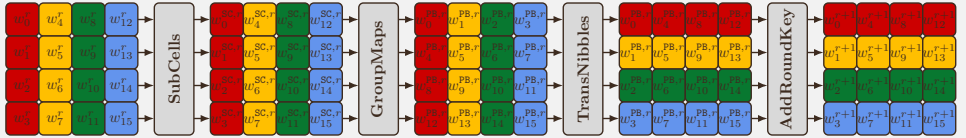


Alternative Description for the Round Function

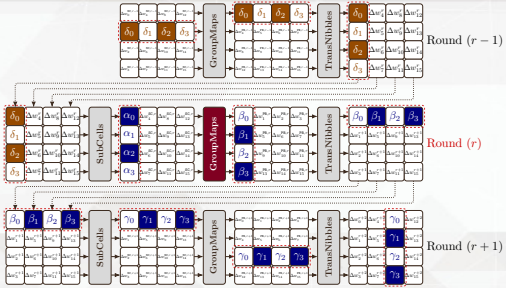
Bit-oriented description



Nibble-oriented description

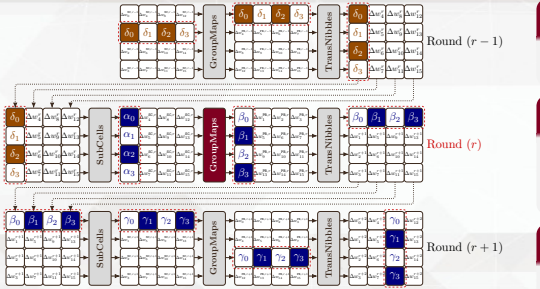


Characteristics with Two Active S-boxes Per Round



$$\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathbf{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3$$

Characteristics with Two Active S-boxes Per Round



$$\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathbf{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3$$

Condition 1

- $\beta_0\|\beta_1\|\beta_2\|\beta_3$ has two nonzero nibbles.

Condition 2

- Two nonzero nibbles in $\beta_0\|\beta_1\|\beta_2\|\beta_3$ cannot take values from the set $\{0x2, 0x4, 0x8\}$.

Condition 3

- Two nonzero nibbles in $\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3$ cannot take values from the set $\{0x1, 0x2, 0x4\}$.

Condition 4

- Denote β_i and β_j the two nonzero nibbles in $\beta_0\|\beta_1\|\beta_2\|\beta_3$, where $i, j \in \{0, 1, 2, 3\}$ and $i \neq j$. Let $\mathcal{S}_i^D$ and $\mathcal{S}_j^D$ be the sets of 1-bit output differences that can be propagated from β_i and β_j, respectively. Then, $\mathcal{S}_i^D \cap \mathcal{S}_j^D \neq \emptyset$ must hold.

Characteristics with Two Active S-boxes Per Round

Proposition 3

- For an R-round differential characteristic activating two S-boxes per round, if the two active S-boxes in the r-th round are located in the same column, then, for all i with $0 \leqslant r + 2 \cdot i < R$, the two active S-boxes in the $(r + 2 \cdot i)$-th round are also located in the same column.

Characteristics with Two Active S-boxes Per Round

Proposition 3

- For an R-round differential characteristic activating two S-boxes per round, if the two active S-boxes in the r-th round are located in the same column, then, for all i with $0 \leqslant r + 2 \cdot i < R$, the two active S-boxes in the $(r + 2 \cdot i)$-th round are also located in the same column.

Lemma 1

- For GIFT-64, if a differential characteristic activates two S-boxes per round, then the two active S-boxes in one of the first two rounds must be located in the same column of the matrix state.

Characteristics with Two Active S-boxes Per Round

Proposition 3

- For an R-round differential characteristic activating two S-boxes per round, if the two active S-boxes in the r-th round are located in the same column, then, for all i with $0 \leqslant r + 2 \cdot i < R$, the two active S-boxes in the $(r + 2 \cdot i)$-th round are also located in the same column.

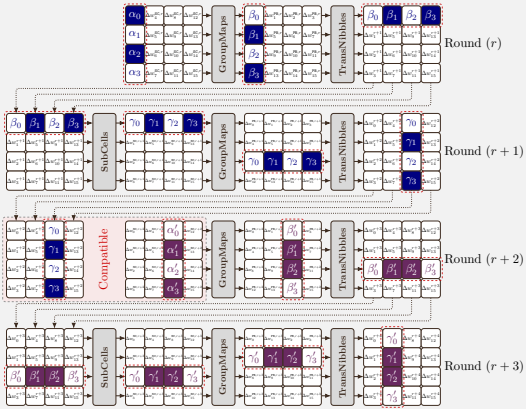
Lemma 1

- For GIFT-64, if a differential characteristic activates two S-boxes per round, then the two active S-boxes in one of the first two rounds must be located in the same column of the matrix state.

Decomposing characteristics with two active S-boxes per round

- All these characteristics can be decomposed into several pieces of 2-round characteristics.
- The two active S-boxes in the first round are located in the same column.
- Differential propagations $\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathrm{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3 \xrightarrow{GS} \gamma_0\|\gamma_1\|\gamma_2\|\gamma_3$ fulfil four conditions.

Constructing characteristics with two active S-boxes per round



$$\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathsf{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3 \xrightarrow{GS} \gamma_0\|\gamma_1\|\gamma_2\|\gamma_3$$

$$\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3 \xrightarrow{\mathsf{g}_0} \beta'_0\|\beta'_1\|\beta'_2\|\beta'_3 \xrightarrow{GS} \gamma'_0\|\gamma'_1\|\gamma'_2\|\gamma'_3$$

- $\gamma_i \xrightarrow{GS} \alpha'_i$ are possible transitions.

Constructing characteristics with two active S-boxes per round

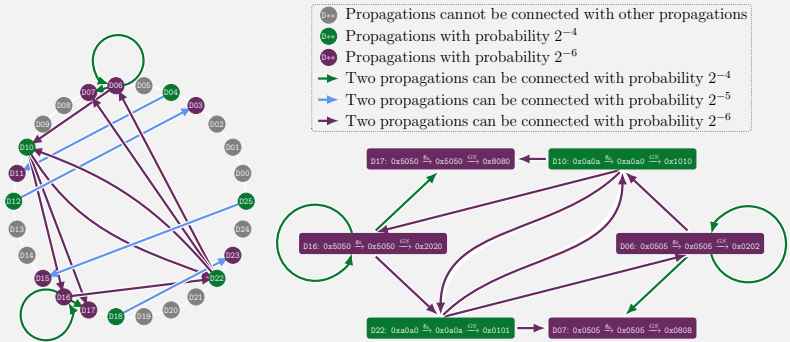
$$\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathsf{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3 \xrightarrow{GS} \gamma_0\|\gamma_1\|\gamma_2\|\gamma_3$$

$$\alpha'_0\|\alpha'_1\|\alpha'_2\|\alpha'_3 \xrightarrow{\mathsf{g}_0} \beta'_0\|\beta'_1\|\beta'_2\|\beta'_3 \xrightarrow{GS} \gamma'_0\|\gamma'_1\|\gamma'_2\|\gamma'_3$$

- $\gamma_i \xrightarrow{GS} \alpha'_i$ are possible transitions.
- Candidate propagations.

Index	$\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathsf{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3 \xrightarrow{GS} \gamma_0\|\gamma_1\|\gamma_2\|\gamma_3$	Probability	Index	$\alpha_0\|\alpha_1\|\alpha_2\|\alpha_3 \xrightarrow{\mathsf{g}_0} \beta_0\|\beta_1\|\beta_2\|\beta_3 \xrightarrow{GS} \gamma_0\|\gamma_1\|\gamma_2\|\gamma_3$	Probability
D00	0x0039 $\xrightarrow{\mathsf{g}_0}$ 0x9003 $\xrightarrow{GS}$ 0x8008	2^{-6}	D13	0x3900 $\xrightarrow{\mathsf{g}_0}$ 0x0390 $\xrightarrow{GS}$ 0x0880	2^{-6}
D01	0x0085 $\xrightarrow{\mathsf{g}_0}$ 0x0c01 $\xrightarrow{GS}$ 0x0808	2^{-6}	D14	0x5008 $\xrightarrow{\mathsf{g}_0}$ 0xc010 $\xrightarrow{GS}$ 0x8080	2^{-6}
D02	0x009c $\xrightarrow{\mathsf{g}_0}$ 0x9c00 $\xrightarrow{GS}$ 0x8800	2^{-6}	D15	0x500a $\xrightarrow{\mathsf{g}_0}$ 0xa030 $\xrightarrow{GS}$ 0x8080	2^{-6}
D03	0x00a5 $\xrightarrow{\mathsf{g}_0}$ 0x0c03 $\xrightarrow{GS}$ 0x0808	2^{-6}	D16	0x5050 $\xrightarrow{\mathsf{g}_0}$ 0x5050 $\xrightarrow{GS}$ 0x2020	2^{-6}
D04	0x00c6 $\xrightarrow{\mathsf{g}_0}$ 0x0c60 $\xrightarrow{GS}$ 0x0220	2^{-4}	D17	0x5050 $\xrightarrow{\mathsf{g}_0}$ 0x5050 $\xrightarrow{GS}$ 0x8080	2^{-6}
D05	0x0390 $\xrightarrow{\mathsf{g}_0}$ 0x3900 $\xrightarrow{GS}$ 0x8800	2^{-6}	D18	0x600c $\xrightarrow{\mathsf{g}_0}$ 0xc600 $\xrightarrow{GS}$ 0x2200	2^{-4}
D06	0x0505 $\xrightarrow{\mathsf{g}_0}$ 0x0505 $\xrightarrow{GS}$ 0x0202	2^{-6}	D19	0x8500 $\xrightarrow{\mathsf{g}_0}$ 0x010c $\xrightarrow{GS}$ 0x0808	2^{-6}
D07	0x0505 $\xrightarrow{\mathsf{g}_0}$ 0x0505 $\xrightarrow{GS}$ 0x0808	2^{-6}	D20	0x9003 $\xrightarrow{\mathsf{g}_0}$ 0x0039 $\xrightarrow{GS}$ 0x0088	2^{-6}
D08	0x0850 $\xrightarrow{\mathsf{g}_0}$ 0x10c0 $\xrightarrow{GS}$ 0x8080	2^{-6}	D21	0x9c00 $\xrightarrow{\mathsf{g}_0}$ 0x009c $\xrightarrow{GS}$ 0x0088	2^{-6}
D09	0x09c0 $\xrightarrow{\mathsf{g}_0}$ 0x09c0 $\xrightarrow{GS}$ 0x0880	2^{-6}	D22	0xa0a0 $\xrightarrow{\mathsf{g}_0}$ 0x0a0a $\xrightarrow{GS}$ 0x0101	2^{-4}
D10	0x0a0a $\xrightarrow{\mathsf{g}_0}$ 0xa0a0 $\xrightarrow{GS}$ 0x1010	2^{-4}	D23	0xa500 $\xrightarrow{\mathsf{g}_0}$ 0x030c $\xrightarrow{GS}$ 0x0808	2^{-6}
D11	0x0a50 $\xrightarrow{\mathsf{g}_0}$ 0x30c0 $\xrightarrow{GS}$ 0x8080	2^{-6}	D24	0xc009 $\xrightarrow{\mathsf{g}_0}$ 0xc009 $\xrightarrow{GS}$ 0x8008	2^{-6}
D12	0x0c60 $\xrightarrow{\mathsf{g}_0}$ 0x00c6 $\xrightarrow{GS}$ 0x0022	2^{-4}	D25	0xc600 $\xrightarrow{\mathsf{g}_0}$ 0x600c $\xrightarrow{GS}$ 0x2002	2^{-4}

Compatibilities among 26 candidate differential propagations



(a) Graph for all 26 propagations.

(b) Six propagations participating in cycles.

Cycles in the graph

- Theoretically explain the existence of long characteristics with two active S-boxes per round.
- Any characteristics for more than seven rounds with two active S-boxes per round.

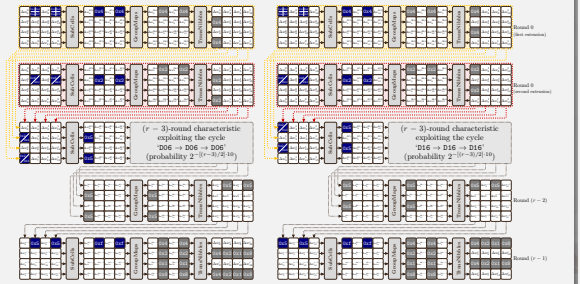
Enumerating All Optimal Differential Characteristics

Explicit formula for the differential probability of the optimal characteristic

- The probability $\Pr(r)$ of r-round optimal differential characteristics with $r \geqslant 8$

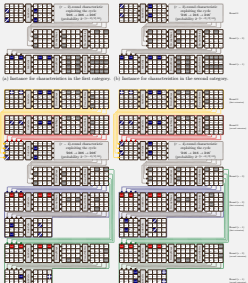
$$-\log_2\big(\Pr(r)\big) = \begin{cases} [(r-3)/2] \cdot 10 + 12 & \text{if } r \bmod 2 \equiv 1, \\ [(r-2)/2] \cdot 10 + 8 & \text{otherwise.} \end{cases}$$

288 optimal trails with $r \bmod 2 \equiv 1$



(a) Instance for characteristics in the first category. (b) Instance for characteristics in the second category.

10400 optimal trails with $r \bmod 2 \equiv 0$



(a) Instance for characteristics in the first category. (b) Instance for characteristics in the second category.
(c) Instance for characteristics in the third category. (d) Instance for characteristics in the fourth category.

Optimal Linear Characteristic of GIFT-64

Proposition 4

- If $r \geqslant 10$, then the optimal r-round linear characteristic of GIFT-64 with the minimum number of active S-boxes must activate two S-boxes per round.

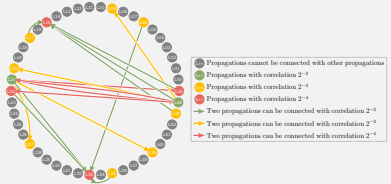
Optimal Linear Characteristic of GIFT-64

Proposition 4

- If $r \geqslant 10$, then the optimal r-round linear characteristic of GIFT-64 with the minimum number of active S-boxes must activate two S-boxes per round.

Constructing linear characteristics with two active S-boxes per round

Index	$\zeta_0 \Vert \zeta_1 \Vert \zeta_2 \Vert \zeta_3 \xrightarrow{E_r} \eta_0 \Vert \eta_1 \Vert \eta_2 \Vert \eta_3 \xrightarrow{GS} \lambda_0 \Vert \lambda_1 \Vert \lambda_2 \Vert \lambda_3$	Correlation
L00	0x0038 $\xrightarrow{E_0}$ 0x9002 $\xrightarrow{GS}$ 0x8008	2^{-3}
L01	0x0039 $\xrightarrow{E_1}$ 0x9003 $\xrightarrow{GS}$ 0x4004	2^{-4}
L02	0x0039 $\xrightarrow{E_1}$ 0x9003 $\xrightarrow{GS}$ 0x8008	2^{-3}
L03	0x0043 $\xrightarrow{E_2}$ 0x0061 $\xrightarrow{GS}$ 0x0044	2^{-3}
L04	0x0043 $\xrightarrow{E_2}$ 0x0061 $\xrightarrow{GS}$ 0x0088	2^{-3}
L05	0x005a $\xrightarrow{E_3}$ 0x9060 $\xrightarrow{GS}$ 0x4040	2^{-3}
L06	0x005a $\xrightarrow{E_3}$ 0x9060 $\xrightarrow{GS}$ 0x8080	2^{-3}
L07	0x0063 $\xrightarrow{E_3}$ 0x0063 $\xrightarrow{GS}$ 0x0044	2^{-3}
L08	0x0063 $\xrightarrow{E_3}$ 0x0063 $\xrightarrow{GS}$ 0x0088	2^{-4}
L09	0x0308 $\xrightarrow{E_4}$ 0xa100 $\xrightarrow{GS}$ 0x8800	2^{-3}
L10	0x0380 $\xrightarrow{E_4}$ 0x2900 $\xrightarrow{GS}$ 0x8800	2^{-3}
L11	0x0390 $\xrightarrow{E_4}$ 0x3900 $\xrightarrow{GS}$ 0x4400	2^{-4}
L12	0x0390 $\xrightarrow{E_4}$ 0x3900 $\xrightarrow{GS}$ 0x8800	2^{-3}
L13	0x0430 $\xrightarrow{E_4}$ 0x1006 $\xrightarrow{GS}$ 0x4004	2^{-3}
L14	0x0430 $\xrightarrow{E_4}$ 0x1006 $\xrightarrow{GS}$ 0x8008	2^{-3}
L15	0x0505 $\xrightarrow{E_5}$ 0x0505 $\xrightarrow{GS}$ 0x0404	2^{-4}
L16	0x05a0 $\xrightarrow{E_5}$ 0x0906 $\xrightarrow{GS}$ 0x0404	2^{-3}
L17	0x05a0 $\xrightarrow{E_5}$ 0x0906 $\xrightarrow{GS}$ 0x0808	2^{-3}
L18	0x0630 $\xrightarrow{E_5}$ 0x3006 $\xrightarrow{GS}$ 0x4004	2^{-3}
L19	0x0630 $\xrightarrow{E_5}$ 0x3006 $\xrightarrow{GS}$ 0x8008	2^{-4}
L20	0x0803 $\xrightarrow{E_6}$ 0x00a1 $\xrightarrow{GS}$ 0x0088	2^{-3}
L21	0x0a0a $\xrightarrow{E_6}$ 0xa0a0 $\xrightarrow{GS}$ 0x2020	2^{-2}
L22	0x0a0a $\xrightarrow{E_6}$ 0xa0a0 $\xrightarrow{GS}$ 0x8080	2^{-4}
L23	0x3004 $\xrightarrow{E_6}$ 0x0610 $\xrightarrow{GS}$ 0x0440	2^{-3}
L24	0x3004 $\xrightarrow{E_6}$ 0x0610 $\xrightarrow{GS}$ 0x0880	2^{-3}
L25	0x3006 $\xrightarrow{E_6}$ 0x0630 $\xrightarrow{GS}$ 0x0440	2^{-3}
L26	0x3006 $\xrightarrow{E_6}$ 0x0630 $\xrightarrow{GS}$ 0x0880	2^{-4}
L27	0x3080 $\xrightarrow{E_6}$ 0x0a10 $\xrightarrow{GS}$ 0x0880	2^{-3}
L28	0x3800 $\xrightarrow{E_6}$ 0x0290 $\xrightarrow{GS}$ 0x0880	2^{-3}
L29	0x3900 $\xrightarrow{E_6}$ 0x0390 $\xrightarrow{GS}$ 0x0440	2^{-4}
L30	0x3900 $\xrightarrow{E_6}$ 0x0390 $\xrightarrow{GS}$ 0x0880	2^{-3}
L31	0x4300 $\xrightarrow{E_6}$ 0x0100 $\xrightarrow{GS}$ 0x4400	2^{-3}
L32	0x4300 $\xrightarrow{E_6}$ 0x0100 $\xrightarrow{GS}$ 0x8800	2^{-3}
L33	0x5050 $\xrightarrow{E_6}$ 0x5050 $\xrightarrow{GS}$ 0x4040	2^{-4}
L34	0x5a00 $\xrightarrow{E_6}$ 0x6090 $\xrightarrow{GS}$ 0x4040	2^{-3}
L35	0x5a00 $\xrightarrow{E_6}$ 0x6090 $\xrightarrow{GS}$ 0x8080	2^{-3}
L36	0x6300 $\xrightarrow{E_6}$ 0x6300 $\xrightarrow{GS}$ 0x4400	2^{-3}
L37	0x6300 $\xrightarrow{E_6}$ 0x6300 $\xrightarrow{GS}$ 0x8800	2^{-4}
L38	0x8003 $\xrightarrow{E_6}$ 0x0029 $\xrightarrow{GS}$ 0x0088	2^{-3}
L39	0x8030 $\xrightarrow{E_6}$ 0x100a $\xrightarrow{GS}$ 0x8008	2^{-3}
L40	0x9003 $\xrightarrow{E_6}$ 0x0039 $\xrightarrow{GS}$ 0x0044	2^{-4}
L41	0x9003 $\xrightarrow{E_6}$ 0x0039 $\xrightarrow{GS}$ 0x0088	2^{-3}
L42	0xa005 $\xrightarrow{E_6}$ 0x0609 $\xrightarrow{GS}$ 0x0404	2^{-3}
L43	0xa005 $\xrightarrow{E_6}$ 0x0609 $\xrightarrow{GS}$ 0x0808	2^{-3}
L44	0xa0a0 $\xrightarrow{E_6}$ 0x0a0a $\xrightarrow{GS}$ 0x0202	2^{-2}
L45	0xa0a0 $\xrightarrow{E_6}$ 0x0a0a $\xrightarrow{GS}$ 0x0808	2^{-4}



(a) Graph for all 46 linear propagations.

(b) Graph for 10 linear propagations related to the cycle.

Outline

- Motivation.
- Preliminaries.
- Differential and Linear Properties of GIFT-64.
- **Can We Improve GIFT-64?**
- Conclusion.

Classifying the Variants of GIFT-64

Candidate variants

- 2304 group mappings $\Rightarrow$ 2304 candidate variants.
- Comparable upper bounds on the differential probability and the linear correlation.

Classifying the Variants of GIFT-64

Candidate variants

- 2304 group mappings $\Rightarrow$ 2304 candidate variants.
- Comparable upper bounds on the differential probability and the linear correlation.

Proposition 7

- Let $\texttt{GIFT-64}[\mathrm{g}_1]$ and $\texttt{GIFT-64}[\mathrm{g}_2]$ be two GIFT-64-like ciphers respectively instantiated with group mappings g_1 and g_2. If there exists an element $\varrho \in \mathbb{P}$ such that $\mathtt{GM}_{\mathrm{g}_2} = \mathtt{RT}_{\varrho} \circ \mathtt{GM}_{\mathrm{g}_1} \circ \mathtt{RT}_{\varrho^{-1}}$, then $\texttt{GIFT-64}[\mathrm{g}_1]$ and $\texttt{GIFT-64}[\mathrm{g}_2]$ differ only by a permutation on the plaintext and ciphertext and a corresponding permutation of the round keys.

Classifying the Variants of GIFT-64

Candidate variants

- 2304 group mappings $\Rightarrow$ 2304 candidate variants.
- Comparable upper bounds on the differential probability and the linear correlation.

Proposition 7

- Let GIFT-64$[\mathrm{g}_1]$ and GIFT-64$[\mathrm{g}_2]$ be two GIFT-64-like ciphers respectively instantiated with group mappings g_1 and g_2. If there exists an element $\varrho \in \mathbb{P}$ such that $\mathtt{GM}_{\mathrm{g}_2} = \mathtt{RT}_{\varrho} \circ \mathtt{GM}_{\mathrm{g}_1} \circ \mathtt{RT}_{\varrho^{-1}}$, then GIFT-64$[\mathrm{g}_1]$ and GIFT-64$[\mathrm{g}_2]$ differ only by a permutation on the plaintext and ciphertext and a corresponding permutation of the round keys.

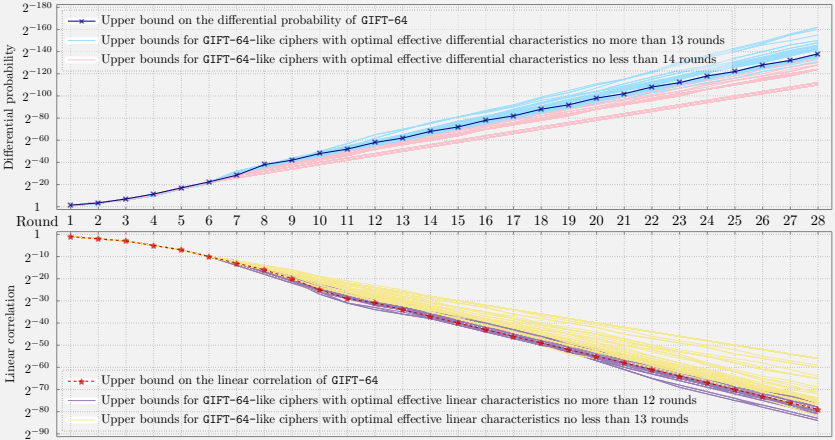
Definition 3 ($\mathbb{GM}$-equivalence)

- Given two elements $\mathtt{GM}_{\mathrm{g}_1}$ and $\mathtt{GM}_{\mathrm{g}_2}$ of the set $\mathbb{GM}$, $\mathtt{GM}_{\mathrm{g}_1}$ and $\mathtt{GM}_{\mathrm{g}_2}$ are called $\mathbb{GM}$-equivalence, if there exists a $\varrho \in \mathbb{P}$ such that $\mathtt{GM}_{\mathrm{g}_2} = \mathtt{RT}_{\varrho} \circ \mathtt{GM}_{\mathrm{g}_1} \circ \mathtt{RT}_{\varrho^{-1}}$. In symbols, $\mathtt{GM}_{\mathrm{g}_1} \sim \mathtt{GM}_{\mathrm{g}_2}$.

- The set of 2304 GIFT-64-like ciphers is partitioned into 168 equivalence classes.
- The number of candidates is reduced from 2303 to 167.

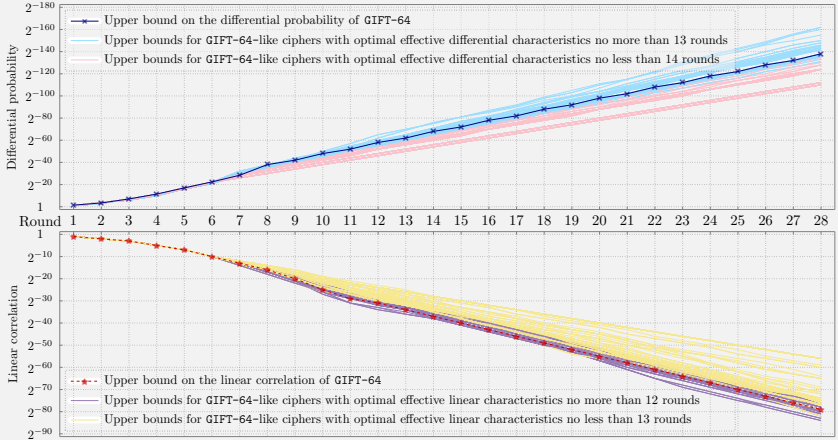
Test Results for 167 Representatives

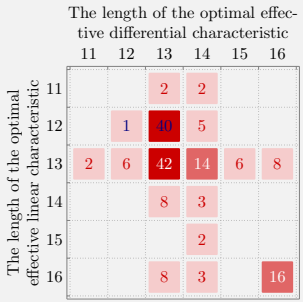
- The security of GIFT-64 against the differential cryptanalysis is moderate.
- The capability of GIFT-64 against linear cryptanalysis is almost among the best of candidates.



Test Results for 167 Representatives

- The security of GIFT-64 against the differential cryptanalysis is moderate.
- The capability of GIFT-64 against linear cryptanalysis is almost among the best of candidates.

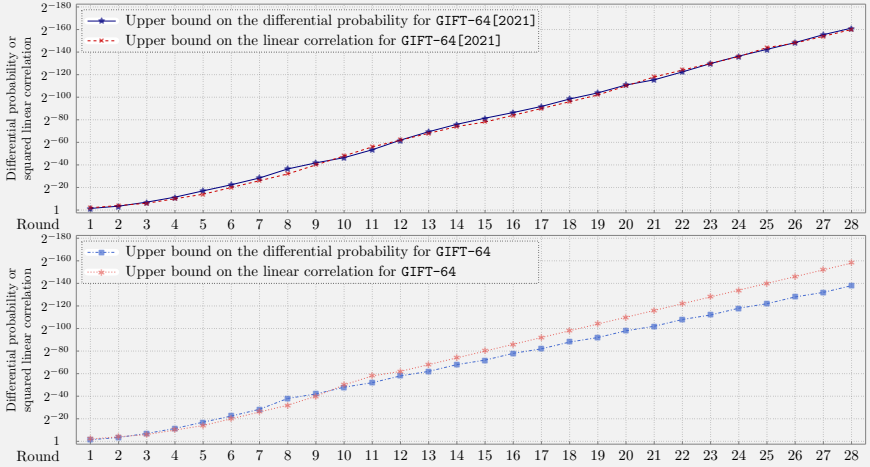




- GIFT-64[2021].

Properties of Variants in GIFT-64[2021]

- The equivalence class GIFT-64[2021] contains 24 elements.
- All variants share the same differential and linear properties.



Properties of Variants in GIFT-64[2021]

- The differential and linear hull properties of GIFT-64[2021] are not significant.
- The security levels of the variants withstanding impossible differential attack, zero-correlation linear attack, and integral attack are similar to those of GIFT-64.

Method	GIFT-64				GIFT-64$[g_0^c]$			
	Round	Time	Data	Memory	Round	Time	Data	Memory
Differential	20	$2^{125.50}$	$2^{62.58}$	$2^{62.58}$	18	$2^{125.16}$	$2^{62.27}$	$2^{62.27}$
Linear	19	$2^{127.11}$	$2^{62.96}$	$2^{60.00}$	18	$2^{126.60}$	$2^{62.96}$	$2^{53.00}$
Integral	14	$2^{97.00}$	$2^{63.00}$	-	14	$2^{97.00}$	$2^{63.00}$	-
ID	6	-	-	-	6	-	-	-

Properties of Variants in GIFT-64[2021]

- The differential and linear hull properties of GIFT-64[2021] are not significant.
- The security levels of the variants withstanding impossible differential attack, zero-correlation linear attack, and integral attack are similar to those of GIFT-64.

Method	GIFT-64				GIFT-64[g_0^c]			
	Round	Time	Data	Memory	Round	Time	Data	Memory
Differential	20	$2^{125.50}$	$2^{62.58}$	$2^{62.58}$	18	$2^{125.16}$	$2^{62.27}$	$2^{62.27}$
Linear	19	$2^{127.11}$	$2^{62.96}$	$2^{60.00}$	18	$2^{126.60}$	$2^{62.96}$	$2^{53.00}$
Integral	14	$2^{97.00}$	$2^{63.00}$	-	14	$2^{97.00}$	$2^{63.00}$	-
ID	6	-	-	-	6	-	-	-

- For the variant GIFT-64[g_0^c], 26 rounds could be used rather than 28 rounds.

	Area (GE)	Delay (ns)	Cycle	TP_{MAX} (MBit/s)	Power (μW)	Energy (pJ)
GIFT-64[g_0^c]	1769	0.55	26	4475.5	36.7	95.4
GIFT-64	1770	0.56	28	4081.6	36.7	102.7
SKINNY-64-128	1804	0.86	36	2067.2	36.8	132.5
SIMON-64-128	1829	0.81	44	1795.7	36.5	160.5

Outline

- Motivation.
- Preliminaries.
- Differential and Linear Properties of GIFT-64.
- Can We Improve GIFT-64?
- **Conclusion.**

Conclusion

Contribution

- Automatic methods & mathematical analysis.
- GIFT-64.
  - Properties of differential characteristics activating two S-boxes per round.
  - All optimal differential characteristics.
  - Properties of linear characteristics with two active S-boxes per round.
- GIFT-64[2021].
  - Variants with comparable differential and linear properties.
  - Resistance against other attacks.

Conclusion

Contribution

- Automatic methods & mathematical analysis.
- GIFT-64.
  - Properties of differential characteristics activating two S-boxes per round.
  - All optimal differential characteristics.
  - Properties of linear characteristics with two active S-boxes per round.
- GIFT-64[2021].
  - Variants with comparable differential and linear properties.
  - Resistance against other attacks.

Future work

- The resistance of variants regarding related-key differential attack can be lifted.
- What if the group mappings operating on different columns are distinct?
- New variants for GIFT-128.

Thank you for your attention!

Thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.