RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: CRYP-R09

MILP-based Differential Attack on Round-reduced GIFT

Speaker: Kai Hu
Key Lab of Cryptologic Technology & Information Security, Ministry of Education, Shandong University
Author: Baoyu Zhu, Xiaoyang Dong, Hongbo Yu

Outline

- Introduction
  - Description of GIFT
- 19-round differential attack for GIFT-64
  - H-representation of the convex hull of GIFT S-box
  - 12-round differential characteristic of GIFT-64
  - 19-round differential attack for GIFT-64
- 23-round differential attack for GIFT-128
  - 18-round differential characteristic of GIFT-128

Outline

- Introduction
  - Description of GIFT
- 19-round differential attack for GIFT-64
  - H-representation of the convex hull of GIFT S-box
  - 12-round differential characteristic of GIFT-64
  - 19-round differential attack for GIFT-64
- 23-round differential attack for GIFT-128
  - 18-round differential characteristic of GIFT-128

Description of GIFT

- A lightweight block cipher proposed by Banik et al. at CHES 2017
- Two versions: GIFT-64 and GIFT-128
  - Block size: 64/128
  - Key size: 128/128
  - Number of rounds: 28/40
  - Structure: SPN structure

Description of GIFT

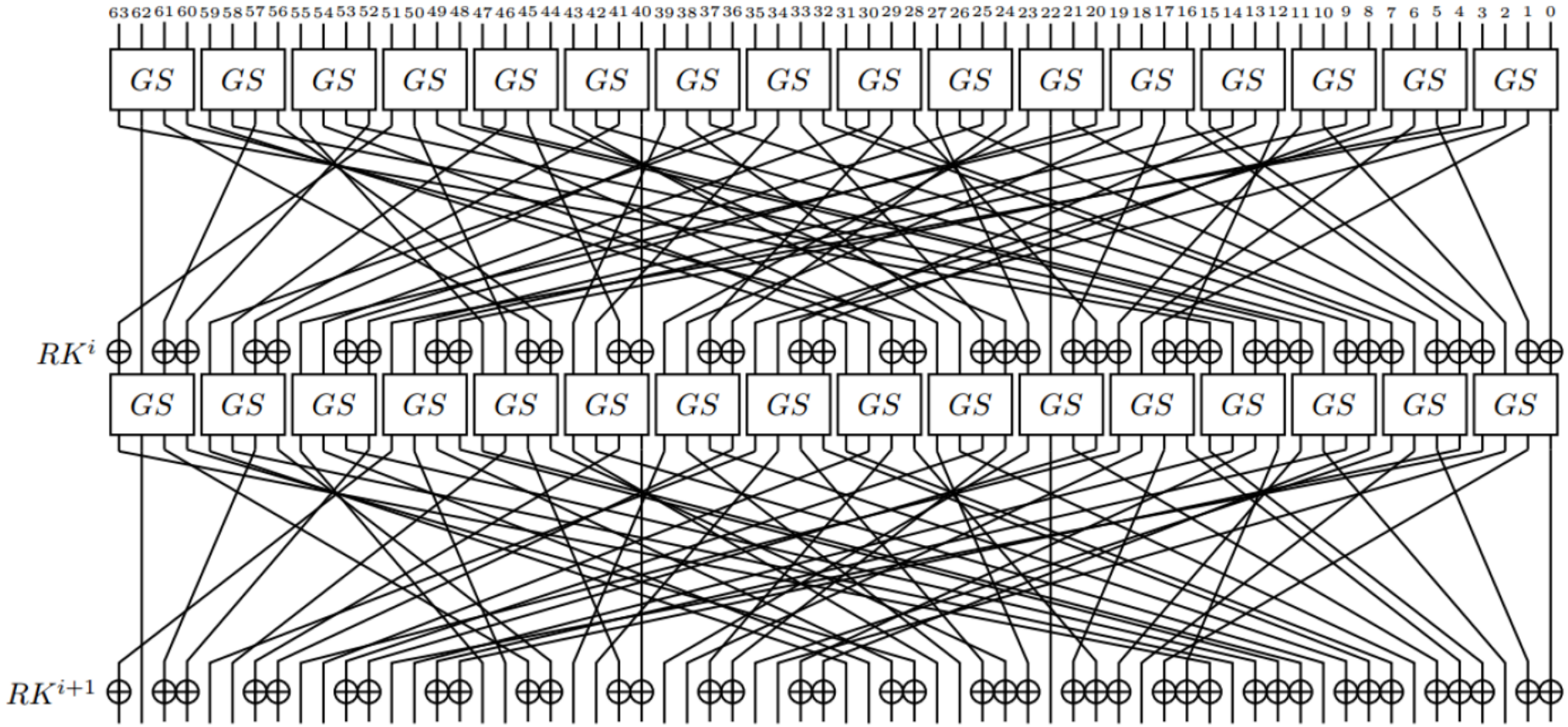
- 4-bit S-box of GIFT

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

- Permutation
  - The input and output of permutation layer are bijective.

Description of GIFT

- Two rounds of GIFT-64



Description of GIFT

- Summary of cryptography analysis on GIFT

	Type	Rounds	Time	Memory	Data	Source
GIFT-64	Integral	14	2^{96}	2^{63}	2^{63}	[BPP+17a]
GIFT-64	MitM	15	2^{120}	2^{8}	2^{64}	[BPP+17a]
GIFT-64	MitM	15	2^{112}	2^{16}	2^{64}	[Yu18]
GIFT-64	Differential	19	2^{112}	2^{80}	2^{63}	Ours
GIFT-128	Differential	23	2^{120}	2^{86}	2^{120}	Ours

[BPP+17a] 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 (2017)
[Yu18] Sasaki, Y.: Integer Linear Programming for Three-Subset Meet-in-the-Middle Attacks: Application to {GIFT}. In: Advances in Information and Computer Security - 13th International Workshop on Security, {IWSEC} 2018, Sendai, Japan, September 3-5, 2018, Proceedings. pp. 227--243 (2018)

Outline

- Introduction
  - Description of GIFT
- 19-round differential attack for GIFT-64
  - H-representation of the convex hull of GIFT S-box
  - 12-round differential characteristic of GIFT-64
  - 19-round differential attack for GIFT-64
- 23-round differential attack for GIFT-128
  - 18-round differential characteristic of GIFT-128

H-representation of the convex hull of GIFT S-box

- Suppose $p = (x_0, x_1, \cdots, x_{w-1}, y_0, y_1, \cdots, y_{v-1})$ is a differential pattern of a $w \times v$ S-box.
- The set of all the differential patterns of S-box can be described with a system of inequalities. The system of inequalities is called the H-Representation of the convex hull[SHW+14].

$$\begin{cases} \alpha_{0,0}x_0 + \alpha_{0,1}x_1 + \cdots + \alpha_{0,w-1}x_{w-1} + \beta_{0,0}y_0 + \beta_{0,1}y_1 + \cdots + \beta_{0,v-1}y_{v-1} + \gamma_0 \geq 0 \\ \vdots \\ \alpha_{n-1,0}x_0 + \alpha_{n-1,1}x_1 + \cdots + \alpha_{n-1,w-1}x_{w-1} + \beta_{n-1,0}y_0 + \beta_{n-1,1}y_1 + \cdots + \beta_{n-1,v-1}y_{v-1} + \gamma_{n-1} \geq 0 \end{cases}$$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	2	0	2	2	2	2	2	0	0	2	
2	0	0	0	0	4	4	0	0	2	2	0	0	2	2	0	
3	0	0	0	0	2	2	0	2	0	0	2	2	2	2	2	
4	0	0	0	2	0	4	0	6	0	2	0	0	0	2	0	0
5	0	0	2	0	0	2	0	0	2	0	0	0	2	2	2	4
6	0	0	4	6	0	0	0	2	0	0	2	0	0	0	2	0
7	0	0	2	0	0	2	0	0	2	2	2	4	2	0	0	0
8	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4
9	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0
a	0	4	0	0	0	4	0	0	2	2	0	0	2	2	0	0
b	0	2	0	2	0	0	2	2	2	2	0	0	2	0	2	0
c	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2	0
d	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
e	0	4	0	0	4	0	0	0	2	2	0	0	2	2	0	0
f	0	2	2	0	4	0	0	0	0	2	0	2	0	0	2	2

DDT of GIFT S-box

[SHW+14]]Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In International Conference on the Theory and Application of Cryptology and Information Security, pages 158–178. Springer, 2014.

H-representation of the convex hull of GIFT S-box

Ninety-nine possible differential patterns in DDT of GIFT S-box $(x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3)$

[SAG]

$$\begin{cases} \alpha_{0,0}x_0 + \alpha_{0,1}x_1 + \alpha_{0,2}x_2 + \alpha_{0,3}x_3 + \beta_{0,0}y_0 + \beta_{0,1}y_1 + \beta_{0,2}y_2 + \beta_{0,3}y_3 + \gamma_0 \geq 0 \\ \vdots \\ \alpha_{236,0}x_0 + \alpha_{236,1}x_1 + \alpha_{236,2}x_2 + \alpha_{236,3}x_3 + \beta_{236,0}y_0 + \beta_{236,1}y_1 + \beta_{236,2}y_2 + \beta_{236,3}y_3 + \gamma_{236} \geq 0 \end{cases}$$

237 inequalities can be generated to constrain the DDT by using Sagemath[SAG].

[SAG] http://www.sagemath

Valid Cutting-off Inequalities from the Convex Hull

$$\begin{cases} Ineq_0 \\ \vdots \\ Ineq_{236} \end{cases} \Longleftrightarrow \begin{cases} IDPatt_0 \\ \vdots \\ IDPatt_{156} \end{cases}$$

237 inequalities

157 impossible Differential Patterns

- For each impossible Differential Pattern $IDPatt_i (0 \le i \le 156)$, it should be excluded by at least one inequality[YT17].

$$\sum_{Ineq_j \text{ } \square IDPatt_i < 0} d_j \ge 1$$

$$\min \sum_{0 \le j \le 236} d_j$$

- Set the objective function to the minimal number of inequalities. Solve this Mix-Integer Linear Programming problem.

[YT17] Sasaki Yu and Yosuke Todo. New algorithm for modeling s-box in milp based differential and division trail search. In International Conference for Information Technology & Communications, 2017.

Differential Patterns with probability

- Differential Patterns with probability

  $(x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3, p_0, p_1, p_2) \in F_2^{8+3}$ defined as follows.

$$\begin{cases} (p_0, p_1, p_2) = (0,0,0), if\ P\left[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)\right] = 1 = 2^{-0} \\ (p_0, p_1, p_2) = (0,0,1), if\ P\left[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)\right] = 6/16 = 2^{-1.415} \\ (p_0, p_1, p_2) = (0,1,0), if\ P\left[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)\right] = 4/16 = 2^{-2} \\ (p_0, p_1, p_2) = (1,0,0), if\ P\left[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)\right] = 2/16 = 2^{-3} \end{cases}$$

- Cutting-off inequalities can be generated just like Differential Patterns without probability.

Two systems of inequalities

$$S_1 \quad \begin{cases} \alpha_{0,0}x_0 + \cdots + \alpha_{0,3}x_3 + \beta_{0,0}y_0 + \cdots + \beta_{0,3}y_3 + \gamma_0 \geq 0 \\ \vdots \\ \alpha_{20,0}x_0 + \cdots + \alpha_{20,3}x_3 + \beta_{20,0}y_0 + \cdots + \beta_{20,3}y_3 + \gamma_{20} \geq 0 \end{cases}$$

21 inequalities to describe the differential pattern of GIFT S-box

$$S_2 \quad \begin{cases} \alpha_{0,0}x_0 + \cdots + \alpha_{0,3}x_3 + \beta_{0,0}y_0 + \cdots + \beta_{0,3}y_3 + \zeta_{0,0}p_0 + \zeta_{0,1}p_1 + \zeta_{0,2}p_2 + \gamma_0 \geq 0 \\ \vdots \\ \alpha_{18,0}x_0 + \cdots + \alpha_{18,3}x_3 + \beta_{18,0}y_0 + \cdots + \beta_{18,3}y_3 + \zeta_{18,0}p_0 + \zeta_{18,1}p_1 + \zeta_{18,2}p_2 + \gamma_{18} \geq 0 \end{cases}$$

19 inequalities to describe the differential pattern with probability of GIFT S-box

Outline

- Introduction
  - Description of GIFT
- 19-round differential attack for GIFT-64
  - H-representation of the convex hull of GIFT S-box
  - 12-round differential characteristic of GIFT-64
  - 19-round differential attack for GIFT-64
- 23-round differential attack for GIFT-128
  - 18-round differential characteristic of GIFT-128

12-round differential characteristic of GIFT-64

- Two-stage search strategy to find differential characteristics of block ciphers is used in [FJP13b][GMS16][SGL+17].
- *In the first step*, we find truncated differential characteristics with mininal number of S-box.
- *In the second step*, we find the differential characteristic with highest probability and it should match the truncated differential characteristics.

[FJP13b] Pierre Alain Fouque, Jérémy Jean, and Thomas Peyrin. Structural evaluation of aes and chosen-key distinguisher of 9-round aes-128. 2013.
[GMS16] David Gerault, Marine Minier, and Christine Solnon. Constraint Programming Models for Chosen Key Differential Cryptanalysis. 2016.
[SGL+17] Siwei Sun, David Gerault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, and Lei Hu. Analysis of aes, skinny, and others with constraint programming. IACR Transactions on Symmetric Cryptology, 2017(1):281–306, 2017.

12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Precalculated: the minimum quantity of active S-box in current solution space.
  - Outer-MILP part: find a truncated differential characteristic in current solution space.
  - Inner-MILP part: add the truncated differential characteristic as a constraint and find the differential characteristic with maximal probability.
  - Revised constraint of Outer-MILP part. Go to Outer-MILP Part.

12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Precalculated: the minimum quantity of active S-box in current solution space.

Rounds	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
DC	1	2	3	5	7	10	13	16	18	20	22	24	26
Source	[BPP+17a]									Ours			

Lower bounds for number of active S-boxes of GIFT-64

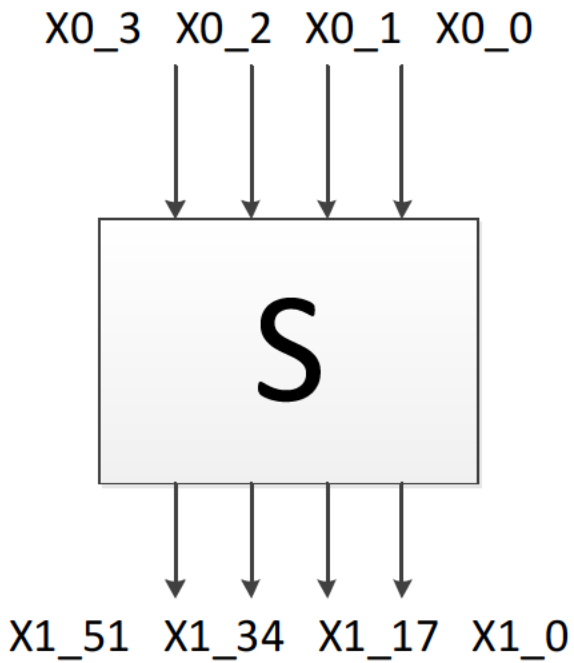
[BPP+17a] Banik, S., Pandey, S.K., Peyrin, T., Sasaki,Y.,Sim,S.M.,Todo,Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In: Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. pp. 321–345 (2017)

12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Outer-MILP part: find a truncated differential characteristic in current solution space.

$$\begin{cases} x_{4i} + x_{4i+1} + x_{4i+2} + x_{4i+3} - a_i \geq 0 \\ a_i - x_{4i} \geq 0 \\ a_i - x_{4i+1} \geq 0 \\ a_i - x_{4i+2} \geq 0 \\ a_i - x_{4i+3} \geq 0 \end{cases}$$

If the i-th S-box is active, $a_i = 1$.

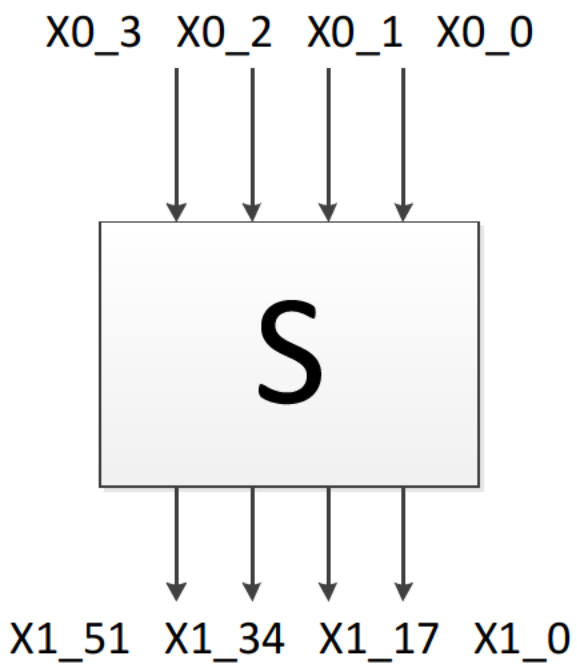


12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Outer-MILP part: find a truncated differential characteristic in current solution space.

We use S_1 to describe the differential characterstic in the Outer-MILP part.

$$\begin{cases} \alpha_{0,0}x_{0-0} + \alpha_{0,1}x_{0-1} + \alpha_{0,2}x_{0-2} + \alpha_{0,3}x_{0-3} + \beta_{0,0}x_{1-0} + \beta_{0,1}x_{1-17} + \beta_{0,2}x_{1-34} + \beta_{0,3}x_{1-51} + \gamma_0 \geq 0 \\ \vdots \\ \alpha_{20,0}x_{0-0} + \alpha_{20,1}x_{0-1} + \alpha_{20,2}x_{0-2} + \alpha_{20,3}x_{0-3} + \beta_{20,0}x_{1-0} + \beta_{20,1}x_{1-17} + \beta_{20,2}x_{1-34} + \beta_{20,3}x_{1-51} + \gamma_{20} \geq 0 \end{cases}$$



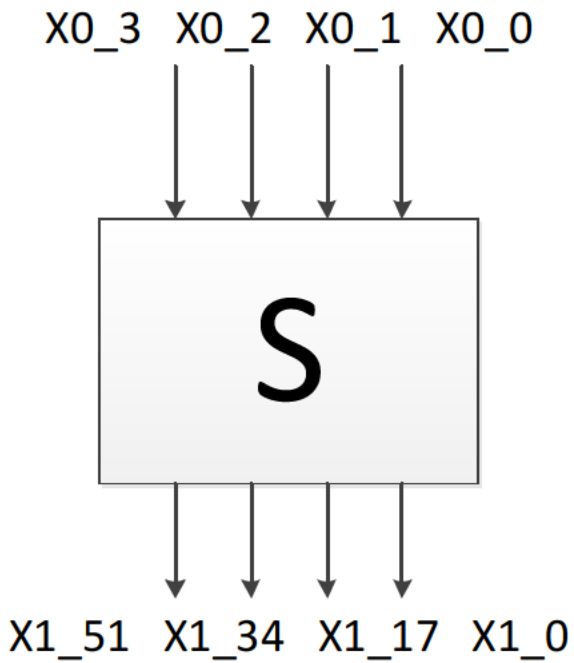
12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Outer-MILP part: find a truncated differential characteristic in current solution space.

The objective function of Outer-MILP part is the number of active S-box.

$$\min \sum_{0 \le i \le 11}^{0 \le j \le 15} a_{i,j}$$

If the objective function reach the minimal quantity of active S-box, send the truncated characteristic to the Inner-MILP part. For 12-round GIFT-64, the lower bound of S-box number is 24.

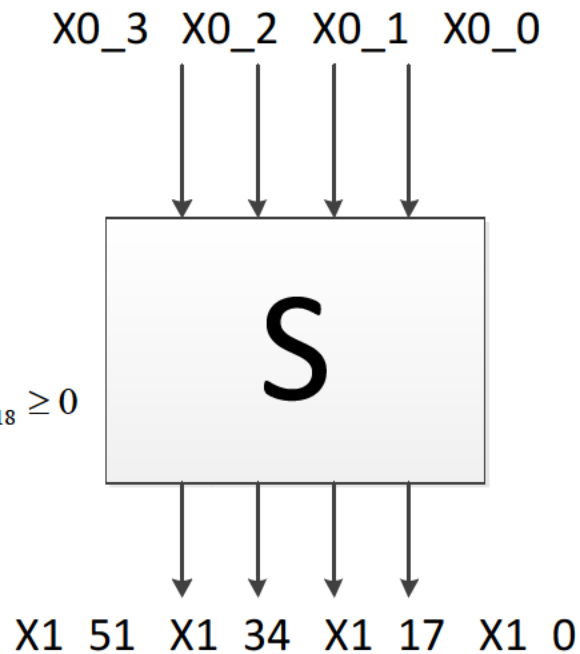


12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Inner-MILP part: add the truncated differential characteristic as a constraint and find the differential characteristic with maximal probability.

We use S_2 to describe the differential characterstic with probability in the Inner-MILP part.

$$\begin{cases} \alpha_{0,0}x_{0-0}+\alpha_{0,1}x_{0-1}+\alpha_{0,2}x_{0-2}+\alpha_{0,3}x_{0-3}+\beta_{0,0}x_{1-0}+\beta_{0,1}x_{1-17}+\beta_{0,2}x_{1-34}+\beta_{0,3}x_{1-51}+\zeta_{0,0}p_{0-0-0}+\zeta_{0,1}p_{0-0-1}+\zeta_{0,2}p_{0-0-2}+\gamma_0 \geq 0 \\ \vdots \\ \alpha_{18,0}x_{0-0}+\alpha_{18,1}x_{0-1}+\alpha_{18,2}x_{0-2}+\alpha_{18,3}x_{0-3}+\beta_{18,0}x_{1-0}+\beta_{18,1}x_{1-17}+\beta_{18,2}x_{1-34}+\beta_{18,3}x_{1-51}+\zeta_{18,0}p_{0-0-0}+\zeta_{18,1}p_{0-0-1}+\zeta_{18,2}p_{0-0-2}+\gamma_{18} \geq 0 \end{cases}$$



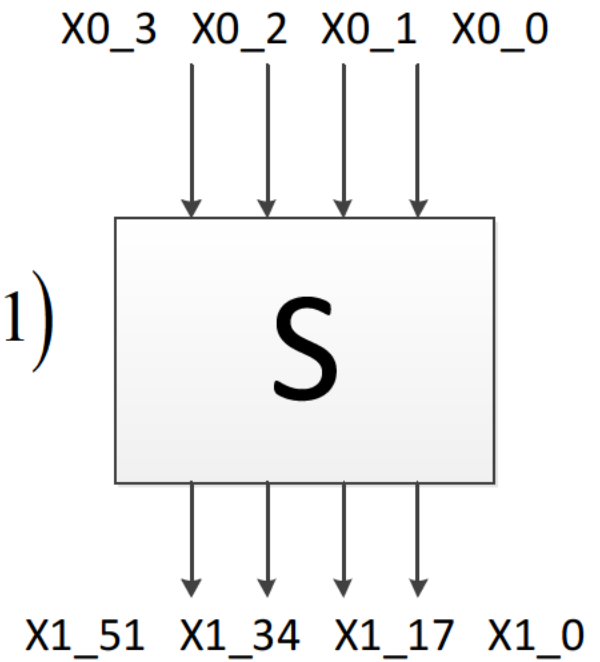
12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Inner-MILP part: add the truncated differential characteristic as a constraint and find the differential characteristic with maximal probability.

The objective function of Inner-MILP part is the probability of differential characteristic.

$$\min \sum_{0\le i\le 11}^{0\le j\le 15} 3\times p_{i,j,0} + 2\times p_{i,j,1} + 1.415\times p_{i,j,2} \qquad \left(a_{i,j}=1\right)$$

If we find the solution, save it and go to the next step.



12-round differential characteristic of GIFT-64

- Algorithm 1 to search for the best differential characteristic of GIFT-64.
  - Revised constraint of Outer-MILP part. Go to Outer-MILP Part.
    - Remove the solution from the feasible space.
    - If we have not got a solution in the feasible space of Outer-MILP part, raise the lower bound for number of active S-boxes and solve it again.

12-round differential characteristic of GIFT-64

- With the help of programming solver *gurobi*[GUR], we get dozens of 12-round differential characteristics with the probability higher or equal to 2^{-60}. The highest probability is 2^{-59}
- We find some of the characteristics are iterative.

Round	Differential-1	Probability
Input	0000 0000 0000 1010	1
1st round	0000 000a 0000 000a	2^{-6}
2nd round	0000 0000 0000 0101	2^{-10}
3rd round	000a 0000 000a 0000	2^{-16}
4th round	0000 0000 0000 1010	2^{-20}

[GUR] http://www.gurobi.com/

Outline

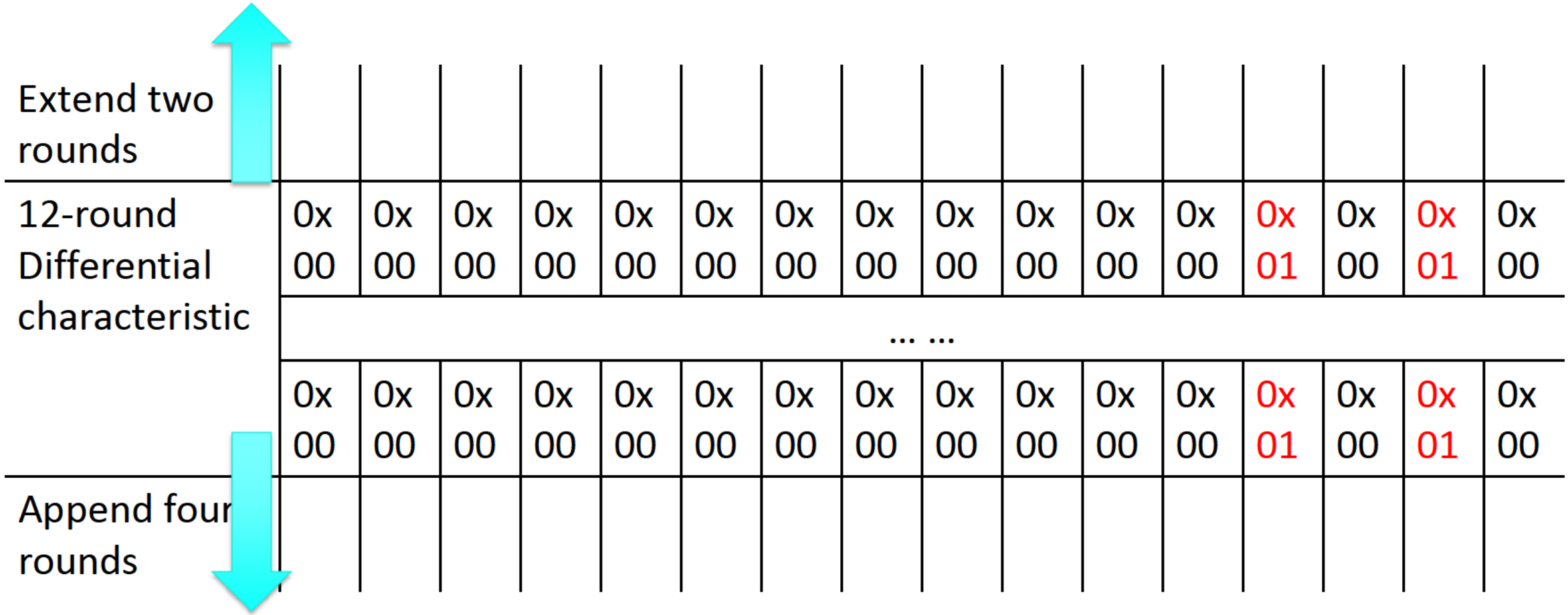
- Introduction
  - Description of GIFT
- 19-round differential attack for GIFT-64
  - H-representation of the convex hull of GIFT S-box
  - 12-round differential characteristic of GIFT-64
  - 19-round differential attack for GIFT-64
- 23-round differential attack for GIFT-128
  - 18-round differential characteristic of GIFT-128

19-round differential attack for GIFT-64

- We use a 12-round differential characteristic to launch a key recovery attack against 19-round GIFT-64. Because active bits in the head and tail of this characteristic is less than others.

Round	Differential	Probability
Input	0000 0000 0000 1010	1
1st round	0000 000a 0000 000a	2^{-6}
2nd round	0000 0000 0000 0101	2^{-10}
3rd round	000a 0000 000a 0000	2^{-16}
4th round	0000 0000 0000 1010	2^{-20}
5th round	0000 000a 0000 000a	2^{-26}
6th round	0000 0000 0000 0101	2^{-30}
7th round	000a 0000 000a 0000	2^{-36}
8th round	0000 0000 0000 1010	2^{-40}
9th round	0000 000a 0000 000a	2^{-46}
10th round	0000 0000 0000 0101	2^{-50}
11th round	000a 0000 000a 0000	2^{-56}
12th round	0000 0000 0000 1010	2^{-60}

19-round differential attack for GIFT-64



19-round differential attack for GIFT-64

- Data Collection
  - Suppose we build 2^n structures after the permutation of the first round. 2^{n+31} pairs can be generated.
  - Each pair has an average probability of 2^{-16} to meet the 4-th round input differential characteristic. The probability of the 12-round differential characteristic is 2^{-60} thus we choose $n = 47$

ΔP	???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????
ΔX_S^1	?000 0?00 00?0 000? ?000 0?00 00?0 000? ?000 0?00 00?0 000? ?000 0?00 00?0 000?
ΔX_P^1	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ???? ???? ???? ????
ΔX_K^1	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ???? ???? ???? ????
ΔX_S^2	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0?0? 10?0 0?0? 10?0
ΔX_P^2	0000 0000 0000 1??? 0000 0000 0000 0000 0000 0000 0000 1??? 0000 0000 0000 0000
ΔX_K^2	0000 0000 0000 1??? 0000 0000 0000 0000 0000 0000 0000 1??? 0000 0000 0000 0000
ΔX_S^3	0000 0000 0000 0001 0000 0000 0000 0000 0000 0000 0000 0001 0000 0000 0000 0000
ΔX_P^3	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 0001 0000
ΔX_K^3	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 0001 0000
4th round input	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 0001 0000

19-round differential attack for GIFT-64

- Key Recovery

  The gussing key bits are generated by the key expansion. We need to construct 2^{80} counters totally. The time complexity is 2^{112}

Round	Key bit
1st round	$k_1^{15}, k_1^{14}, k_1^{13}, k_1^{12}, k_1^{11}, k_1^{10}, k_1^{9}, k_1^{8}, k_1^{7}, k_1^{6}, k_1^{5}, k_1^{4}, k_1^{3}, k_1^{2}, k_1^{1}, k_1^{0}$ $k_0^{15}, k_0^{14}, k_0^{13}, k_0^{12}, k_0^{11}, k_0^{10}, k_0^{9}, k_0^{8}, k_0^{7}, k_0^{6}, k_0^{5}, k_0^{4}, k_0^{3}, k_0^{2}, k_0^{1}, k_0^{0}$
2nd round	$k_3^{15}, k_3^{14}, k_3^{13}, k_3^{12}, k_3^{11}, k_3^{10}, k_3^{9}, k_3^{8}, k_3^{7}, k_3^{6}, k_3^{5}, k_3^{4}, k_3^{3}, k_3^{2}, k_3^{1}, k_3^{0}$ $k_2^{15}, k_2^{14}, k_2^{13}, k_2^{12}, k_2^{11}, k_2^{10}, k_2^{9}, k_2^{8}, k_2^{7}, k_2^{6}, k_2^{5}, k_2^{4}, k_2^{3}, k_2^{2}, k_2^{1}, k_2^{0}$
16th round	$k_7^{5}, k_7^{4}, k_7^{3}, k_7^{2}, k_7^{1}, k_7^{0}, k_7^{15}, k_7^{14}, k_7^{13}, k_7^{12}, k_7^{11}, k_7^{10}, k_7^{9}, k_7^{8}, k_7^{7}, k_7^{6}$ $k_6^{3}, k_6^{2}, k_6^{1}, k_6^{0}, k_6^{15}, k_6^{14}, k_6^{13}, k_6^{12}, k_6^{11}, k_6^{10}, k_6^{9}, k_6^{8}, k_6^{7}, k_6^{6}, k_6^{5}, k_6^{4}$
17th round	$k_1^{7}, k_1^{6}, k_1^{5}, k_1^{4}, k_1^{3}, k_1^{2}, k_1^{1}, k_1^{0}, k_1^{15}, k_1^{14}, k_1^{13}, k_1^{12}, k_1^{11}, k_1^{10}, k_1^{9}, k_1^{8}$ $k_0^{15}, k_0^{14}, k_0^{13}, k_0^{12}, k_0^{11}, k_0^{10}, k_0^{9}, k_0^{8}, k_0^{7}, k_0^{6}, k_0^{5}, k_0^{4}, k_0^{3}, k_0^{2}, k_0^{1}, k_0^{0}$
18th round	$k_3^{7}, k_3^{6}, k_3^{5}, k_3^{4}, k_3^{3}, k_3^{2}, k_3^{1}, k_3^{0}, k_3^{15}, k_3^{14}, k_3^{13}, k_3^{12}, k_3^{11}, k_3^{10}, k_3^{9}, k_3^{8}$ $k_2^{15}, k_2^{14}, k_2^{13}, k_2^{12}, k_2^{11}, k_2^{10}, k_2^{9}, k_2^{8}, k_2^{7}, k_2^{6}, k_2^{5}, k_2^{4}, k_2^{3}, k_2^{2}, k_2^{1}, k_2^{0}$
19th round	$k_5^{7}, k_5^{6}, k_5^{5}, k_5^{4}, k_5^{3}, k_5^{2}, k_5^{1}, k_5^{0}, k_5^{15}, k_5^{14}, k_5^{13}, k_5^{12}, k_5^{11}, k_5^{10}, k_5^{9}, k_5^{8}$ $k_4^{15}, k_4^{14}, k_4^{13}, k_4^{12}, k_4^{11}, k_4^{10}, k_4^{9}, k_4^{8}, k_4^{7}, k_4^{6}, k_4^{5}, k_4^{4}, k_4^{3}, k_4^{2}, k_4^{1}, k_4^{0}$

Outline

- Introduction
  - Description of GIFT
- 19-round differential attack for GIFT-64
  - H-representation of the convex hull of GIFT S-box
  - 12-round differential characteristic of GIFT-64
  - 19-round differential attack for GIFT-64
- 23-round differential attack for GIFT-128
  - 18-round differential characteristic of GIFT-128

18-round differential characteristic of GIFT-128

- GIFT-128 has thirty-two 4-bits S-boxes in each round. It costs too much time to solve it with the Algorithm 1 presented in the previous chapter.
- A segmented MILP-based method can be used to search for longer differential characteristic of GIFT-128.

18-round differential characteristic of GIFT-128

- Search method:
  - Precalculated: the minimum quantity of active S-box for round-reduced cipher.
  - Algorithm 1 mentioned in the previous chapter can be used *repeatedly* to search for longer differential characteristic of GIFT-128.
  - Revised constraint of this model.

18-round differential characteristic of GIFT-128

- Search method:
  - Precalculated: the minimum quantity of active S-box for round-reduced cipher.

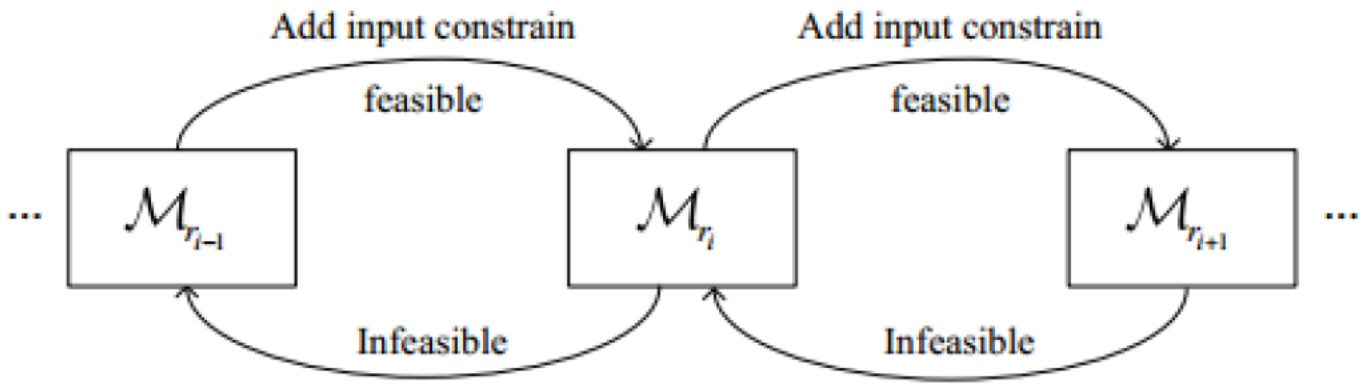
Rounds	1	2	3	4	5	6	7	8	9
DC	1	2	3	5	7	10	13	17	19
Source	[BPP+17a]								

Lower bounds for number of active S-boxes of GIFT-64

[BPP+17a] 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 (2017)

18-round differential characteristic of GIFT-128

- Search method:
  - Algorithm 1 mentioned in the previous chapter can be used *repeatedly* to search for longer differential characteristic of GIFT-128.
    - The length of sub-cipher can neither be too short nor be too long.



18-round differential characteristic of GIFT-128

- Search method:
  - Revised constraint of this model.
    - Remove the solution from the feasible space.

18-round differential characteristic of GIFT-128

- We get a 18-round differential characteristic of GIFT-128 with probability 2^{-109}

Round	Input Difference	Probability
Input	0000 0000 7060 0000 0000 0000 0000 0000	1
1st	0000 0000 0000 0000 0000 0000 00a0 0000	2^{-5}
2nd	0000 0010 0000 0000 0000 0000 0000 0000	2^{-7}
3rd	0000 0000 0800 0000 0000 0000 0000 0000	2^{-10}
4th	0020 0000 0010 0000 0000 0000 0000 0000	2^{-12}
5th	0000 0000 0000 0000 4040 0000 2020 0000	2^{-17}
6th	0000 5050 0000 0000 0000 5050 0000 0000	2^{-25}
7th	0000 0000 0000 0000 0000 0000 0a00 0a00	2^{-37}
8th	0000 0000 0000 0011 0000 0000 0000 0000	2^{-41}
9th	0008 0000 0008 0000 0000 0000 0000 0000	2^{-47}
10th	0000 0000 0000 0000 2020 0000 1010 0000	2^{-51}
11th	0000 5050 0000 0000 0000 5050 0000 0000	2^{-61}
12th	0000 0000 0a00 0a00 0000 0000 0000 0000	2^{-73}
13th	0000 0000 0011 0000 0000 0000 0000 0000	2^{-77}
14th	0090 0000 00c0 0000 0000 0000 0000 0000	2^{-83}
15th	1000 0000 0080 0000 0000 0000 0000 0000	2^{-89}
16th	0010 0000 0000 0000 0000 0000 8020 0000	2^{-94}
17th	0000 0000 8000 0020 0000 0050 0000 0020	2^{-101}
18th	0000 0100 0020 0800 0014 0404 0002 0202	2^{-109}

23-round differential attack for GIFT-128

- We can add three rounds at beginning and two rounds at the end to attack 23-round GIFT-128.
- Time complexity: 2^{120}
- Data complexity: 2^{120}
- Memory complexity: 2^{86}

- All of the source code is uploaded to GitHub (https://github.com/zhuby12/MILP-basedModel)

RSAConference2019

That is all.
Thank you!