MILP Based Differential Attack on Round Reduced WARP

Manoj Kumar and Tarun Yadav

Scientific Analysis Group, DRDO, Metcalfe House Complex, Delhi-110054, INDIA
{manojkumar,tarunyadav}@sag.drdo.in

Abstract. WARP is proposed by S. Banik et al. in SAC 2020. It is a 128-bit lightweight block cipher with 128-bit key. WARP is based on 32-nibble type-2 Generalised Feistel Network (GFN). It uses permutation over nibbles designed to optimize the security and efficiency. Designers have provided a lower bound for the number of differentially active S-boxes but detailed differential characteristics are not provided. In this paper, we discuss MILP based search technique and present differential characteristics for 18-round and 19-round WARP with probability of 2^{-122} and 2^{-132} respectively. To the best of our knowledge, these detailed differential characteristics for WARP are presented for the first time.

Keywords: Lightweight Cryptography, Block Cipher, Differential Cryptanalysis, MILP

1 Introduction

Lightweight cryptography is used for encryption and authentication on small computing devices *e.g.* RFID tags, sensor networks and smart cards [5]. PRESENT is the first notable lightweight block cipher design published in 2007 [3]. There are many lightweight ciphers designed in past two decades. Initially, 64-bit block with 80-bit key was used for designing the lightweight version of block ciphers. Nowadays, 64-bit/128-bit block with 128-bit key is used to design a lightweight block cipher. 128-bit lightweight block ciphers are useful in a sense that it can be used directly in place of AES [4]. NIST has initiated a competition in 2018 to standardise the lightweight cryptographic algorithms seeing the increasing importance of lightweight cryptography.

Differential attack is a basic cryptanalysis technique proposed by E. Biham and A. Shamir [2] in 1990. This exploits the non-uniform relations between the input and output differences. The probability of best differential characteristic is used to provide a bound on the security of block cipher against differential attack. High probability differential characteristics are essential for a successful differential attack. Techniques based on automated search are used to construct these differential characteristics. Matsui[7] proposed a branch-and-bound based technique to search the high probability differential characteristics in 1993. This technique has limitations in searching the differential characteristics for large block sizes. In 2012, N. Mohua et al. [8] proposed a new technique using Mixed

Integer Linear Programming (MILP) to search the differential characteristics efficiently.

MILP deals with optimization problems in which objective function and constraints are linear. There are various commercial linear programming problem (LPP) solvers *e.g.* Gurobi [13] and CPLEX [14]. These solvers provide the solution for an LPP problem very efficiently. Mouha et al. proposed a framework to convert the differential characteristic search problem into an MILP problem and used MILP solvers to provide the characteristics with least number of active S-boxes. At Asiacrypt 2014, Sun et al. [10] applied MILP based attack on bit oriented block ciphers using H-Representation of convex hull for all differential patterns of S-box to find the actual differential characteristics. Differential characteristic search problem is divided into two modules. In first module, a lower bound for the number of differentially active S-boxes is computed. While, differential characteristics with high probability are constructed in second module. Zhu B. et al. presented this kind of differential attack on GIFT [11].

Designers of WARP [1] used MILP-aided search to compute a lower bound for the number of differentially active S-boxes. But, they have not provided the differential characteristics with these bounds. According to their analysis, there are 61 active S-boxes in any 18-round differential characteristics of WARP which can be used for key recovery. This bound for 19 rounds is given as 66 which requires 2^{132} chosen plain text pairs and it is infeasible for 128-bit block cipher. In this paper, we construct differential characteristics for 18-round WARP using MILP-aided search. Firstly, we compute a lower bound on the number of differentially active S-boxes which are equal to the designers bounds. Secondly, we construct the actual differential characteristics for 18-round WARP which can be used for key recovery.

We organise the remaining paper in following manner. In section 2, we provide a brief introduction to lightweight block cipher WARP. In section 3, we we compute a lower bound on the number of differentially active S-boxes and construct 18-round and 19-round differential characteristics using MILP-aided search. The paper is concluded in section 4.

2 Preliminaries

2.1 Description of WARP

The base structure of lightweight block cipher WARP is a type-2 Generalised Feistel Network (GFN) structure. There are many 64-bit block ciphers with 16 branches designed using type-2 GFN structure. But, there is a problem of slow diffusion with 64-bit block and 16 branch ciphers. GFN is revisited by S. Banik *et.al.* [1] and 128-bit block with 32-branches is considered more suitable to design a 128-bit lightweight block cipher.

2.2 Encryption Algorithm:

WARP encrypts 128-bit plaintext block using 128-bit key and generates 128-bit ciphertext block. There are total 41 rounds. Designers have explained the round function of WARP in various equivalent forms. We have used LBlock like equivalent form of WARP to describe its encryption algorithm. Encryption algorithm encrypts 128-bit input X using 128-bit key K. Key expansion algorithm is not required for WARP. Key K is divided into two 64-bit keys K_0 & K_1 and it is expressed as $K = (K_0, K_1)$. In odd rounds, left key K_0 is used and every even round uses right part K_1. We express the 128-bit input X by 32 nibbles from right to left. Then, initial permutation (IP) is applied on X to get two 64-bit words X_{2i} and X_{2i+1} (for $0 \leq i \leq 15$) (Algorithm 1). In each round, constants (Table 2) are XORed with first two nibbles of X^r_{2i+1}. S-box layer (Table 1) is applied on X^r_{2i} by dividing it in 4-bit nibbles. Output from S-box layer is XORed with the round key and nibble permutation (N_P - Table 3) is applied thereafter to get a 64-bit output U. Cyclic rotation by 24 bits is applied on X^r_{2i+1} to get a 64-bit output V. U and V are XORed to get X^{r+1}_{2i} while X^r_{2i} becomes X^{r+1}_{2i+1} due to feistel structure. This process is applied 40 times and the last round is performed without rotation and permutation.

Algorithm 1: Encryption Algorithm

```
Input: $X = (x_{31}, x_{30}, \cdots, x_0)$ and $K = (K_0, K_1)$
Output: $X^{41}$
IP: $X^1_{2i} = (x_0, x_2, \cdots, x_{30})$, $X^1_{2i+1} = (x_1, x_3, \cdots, x_{31})$, where $0 \leq i \leq 15$
for $r$=1 to 40 do
    $X^r_1 = X^r_1 \oplus RC^r_0, X^r_3 = X^r_3 \oplus RC^r_1$
    $Y = S(X^r_{2i})$
    $U = N_P(Y \oplus K_{(r-1)mod2})$
    $V = X^r_{2i+1} <<< 24$
    $X^{r+1}_{2i} = U \oplus V$
    $X^{r+1}_{2i+1} = X^r_{2i}$
end
$X^{41}_1 = X^{40}_1 \oplus RC^{40}_0, X^{41}_3 = X^{40}_3 \oplus RC^{40}_1$
$X^{41}_{2i} = X^{40}_{2i}$
$X^{41}_{2i+1} = S(X^{40}_{2i}) \oplus K_0 \oplus X^{40}_{2i+1}$
```

S-box: The following 4-bit S-box (Table 1) is applied in S-box layer of WARP.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

Table 1: S-Box

Round Constants: In each round, 4-bit round constant given in Table 2 is used:

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
RC_0^r	0	0	1	3	7	f	f	f	e	d	a	5	a	5	b	6	c	9	3	6	d
RC_1^r	4	c	c	c	c	c	8	4	8	4	8	4	c	8	0	4	c	8	4	c	c
r	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	
RC_0^r	b	7	e	d	b	6	d	a	4	9	2	4	9	3	7	e	c	8	1	2	
RC_1^r	8	4	c	8	4	8	0	4	8	0	4	c	c	8	0	0	4	8	4	c	

Table 2: Round Constants

Nibble Permutation: Output from S-box layer is divided into 16 nibbles. Nibble permutation N_P is applied on these 16 nibbles (Table 3).

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$N_P(i)$	3	7	6	4	1	0	2	5	11	15	14	12	9	8	10	13

Table 3: Permutation

3 Differential attack on Round-Reduced WARP

3.1 Differential Cryptanalysis

Differential attack is a powerful cryptanalysis tool proposed by Biham and Shamir against DES [2] in 1990. In this attack, propagation of input differences is studied to find the high probable output differences. These non-random relations are used as distinguisher and round subkeys are constructed using these distinguishers. Therefore, we need a differential characteristic suggesting the particular input and output occurrences with very high probability p for the target cipher. Data complexity of differential attack is inversely proportional to the probability p of differential characteristic. Which means that we need p^{-1} chosen plaintext pairs to distinguish r rounds of an n-bit block cipher. This differential characteristic can be extended to $r+i$ rounds, till the bound $p^{-1} \ggg 2^n$ is satisfied for n-bit block cipher.

3.2 Construction of Differential Characteristics using MILP Model

A high probability differential characteristic is used for key recovery attack by adding some rounds on top and bottom of the trail. There exists several automated techniques to search the optimal differential trails for block ciphers [6]. MILP based technique convert the problem into a linear programming and solve it using the optimization problem solvers. MILP models an inequalities based system with bit variables.

The non-linear function used in a block cipher is S-box. Therefore, we need to write the all possible input and output differences to S-box in linear equations. For this purpose, difference distribution table (DDT) (Appendix - A) of S-box is used. Using SageMath [12], we get 239 inequalities and we reduce this set by removing redundant inequalities with the constraint of impossible differentials present in DDT [9]. We have used Gurobi solver [13] for reduction procedure and we get 21 linear inequalities (Appendix - B) for S-box. The set of 21 inequalities is used to minimize active S-boxes using MILP model. Further, by analysing differential distribution probabilities of S-Box, 1304 inequalities have been generated using SageMath and by applying reduction procedure we get 20 inequalities (Appendix - C). These inequalities are used to minimize probabilities in MILP model. Using these inequalities we first minimize no of S-box and then by minimizing the probabilities we get desired differential characteristics. Differential characteristics for 18-round and 19-round of WARP are described in following subsections.

3.3 Differential Characteristics for 18-round WARP

Using MILP, a 17-round differential characteristics has been constructed with 57 active S-boxes and 2^{-114} probability. This characteristics is extended by adding one round at the top to get 18-round characteristic with 61 active S-boxes and 2^{-122} probability as described in Table 4.

Round Index	Input Difference	Probability (p)
Input	0007a000fa7000000a000000d5f000d0	1
1	00700d00a0000000aa00000050000000	2^{-8}
2	0000d50000000000a000000000000a00	2^{-12}
3	000050000000000a000000000000aa00	2^{-16}
4	00000000000000a0000000000000a000	2^{-20}
5	000000000a00000000000000000a0000	2^{-20}
6	0000000aa0000000000a000000a00000	2^{-24}
7	000000aa00000a0000a00a00000a0000	2^{-28}
8	0a0000a00000af000000a00000a00000	2^{-36}
9	a0000f0a0000f000000a00000a000000	2^{-40}
10	0000f0a00000000a00a0000aaf0f0000	2^{-48}
11	00000a000a0000a00f0500aaf0f00a0a	2^{-56}
12	000aaf0aa000000afa500aa00500ada0	2^{-70}
13	00aaf0a000000aaaa000a00a5000df00	2^{-86}
14	00a00500000fa0aa000a00a0000af000	2^{-96}
15	000050000af000a000a500000aa00000	2^{-106}
16	00000000a000000005500000a000000a	2^{-112}
17	00000a00000000000500000000a0000a5	2^{-116}
18	0000a000000a000f0000000fa7000550	2^{-122}

Table 4: 18-round Differential Characteristics(extension of 17-round)

We have also constructed 18-round differential characteristics without extending lower round characteristic. Although, patterns of active S-boxes and differential probabilities are similar to the characteristics described in Table 4. The another 18-round differential characteristic with 61 active S-boxes and 2^{-122} probability is described in Table 5.

Round Index	Input Difference	Probability (p)
Input	000af000faf000000a0000005f500050	1
1	00a00500a0000000af000000f0000000	2^{-8}
2	00005f0000000000f000000000000a00	2^{-12}
3	0000f0000000000a000000000000af00	2^{-16}
4	00000000000000a0000000000000f000	2^{-20}
5	000000000f00000000000000000a0000	2^{-20}
6	0000000ff0000000000a000000a00000	2^{-24}
7	000000fa00000a0000a00f00000a0000	2^{-28}
8	0a0000a00000aa000000f00000a00000	2^{-36}
9	a0000f0a0000a000000a00000a000000	2^{-40}
10	0000f0a00000000a00a0000aaa050000	2^{-48}
11	00000a000f0000a00f0d00aaa0500a0a	2^{-56}
12	000aaa0af000000affd00aa00d00ada0	2^{-70}
13	00aaa0a0000005aaf000a00ad000df00	2^{-86}
14	00a00d00000a50aa000a00a0000af000	2^{-96}
15	0000d0000aa000a000ad000005a00000	2^{-106}
16	00000000a00000000dd000005000000a	2^{-112}
17	0000050000000000d00000000a0000ad	2^{-116}
18	00005000000a00070000000da7000dd0	2^{-122}

Table 5: 18-round Differential Characteristics

3.4 Differential Characteristics for 19-round WARP

S. Banik [1] has given lower bound on number of active S-boxes till 19-round WARP. We have found a differential characteristics with same number of active S-boxes as the lower bound for 19-round WARP by extending 18-round differential characteristics (Table 4). Table 6 describes the 19-round differential characteristics with 66 active S-boxes and 2^{-132} probability.

Round Index	Input Difference	Probability (p)
Input	0007a000fa7000000a000000d5f000d0	1
1	00700d00a0000000aa00000050000000	2^{-8}
2	0000d50000000000a000000000000a00	2^{-12}
3	000050000000000a000000000000aa00	2^{-16}
4	00000000000000a0000000000000a000	2^{-20}
5	000000000a00000000000000000a0000	2^{-20}
6	0000000aa0000000000a000000a00000	2^{-24}
7	000000aa00000a0000a00a00000a0000	2^{-28}
8	0a0000a00000af000000a00000a00000	2^{-36}
9	a0000f0a0000f000000a00000a000000	2^{-40}
10	0000f0a00000000a00a0000aaf0f0000	2^{-48}
11	00000a000a0000a00f0500aaf0f00a0a	2^{-56}
12	000aaf0aa000000afa500aa00500ada0	2^{-70}
13	00aaf0a000000aaaa000a00a5000df00	2^{-86}
14	00a00500000fa0aa000a00a0000af000	2^{-96}
15	000050000af000a000a500000aa00000	2^{-106}
16	00000000a000000005500000a000000a	2^{-112}
17	00000a0000000000500000000a0000a5	2^{-116}
18	0000a000000a000f0000000fa7000550	2^{-122}
19	000f0a000aa500f00d0000fd70005a00	2^{-132}

Table 6: 19-round Differential Characteristics

4 Conclusion

In this paper, we have presented differential characteristics of WARP using MILP-aided search. We obtained lower bounds on the number of active S-boxes for different rounds which is similar to the designers lower bound. We have also presented detailed differential characteristics using MILP. Differential characteristic for 18-round with 61 active S-boxes and probability of 2^{-122} is constructed. Differential characteristic for 19-round with 66 active S-boxes and probability of 2^{-132} is constructed by extending the 18-round characteristic. We can use 18-round differential characteristic of WARP for key recovery by adding rounds on the top and bottom of the characteristic.

References

1. Banik, S., Bao, Z., Isobe, T., Kubo, H., Minematsu, K., Liu, F., Sakamoto, K., Shibata, N., Shigeri, M.: WARP : Revisiting GFN for Lightweight 128-bit Block Cipher. Selected Areas in Cryptography 2020

2. Biham, E., Shamir, A.: Differential Cryptanalysis of the full 16-round DES, CRYPTO 92, LNCS, Vol. 740, 487–496, Springer, (1992)

3. Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg.

4. Daemen, J., Rijmen, V.: The Design of Rijndael, Springer-Verlag, (2002)

5. Knudsen, L., Robshaw, M.J.B.: Block Cipher Companion, Book Springer, ISBN 978-3-642-17341-7, (2011)

6. Kumar, M., Suresh, TS, Pal, S.K., Panigrahi, A.: Optimal Differential Trails in Lightweight Blokc Ciphers ANU and PICO, Cryptologia, Vol. 44, No. 1, 68–78, (2020)

7. Matsui, M.: On Correlation between the Order of S-boxes and the Strength of DES, EUROCRYPT 94, LNCS, Vol 950, 366–375, Springer, (1994)

8. Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers. 57–76, (2011)

9. Sasaki Y., Todo Y. (2017) New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search. In: Farshim P., Simion E. (eds) Innovative Security Solutions for Information Technology and Communications. SecITC 2017. Lecture Notes in Computer Science, vol 10543. Springer, Cham.

10. Sun S., Hu L., Wang P., Qiao K., Ma X., Song L. (2014) Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers. In: Sarkar P., Iwata T. (eds) Advances in Cryptology – ASIACRYPT 2014. ASIACRYPT 2014. Lecture Notes in Computer Science, vol 8873. Springer, Berlin, Heidelberg.

11. Zhu, B., Dong, X., Yu, H.: MILP-Based Differential Attack on Round-Reduced GIFT. In: Topics in Cryptology - CT-RSA 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings. pp. 372-390, (2019)

12. https://www.sagemath.org/

13. https://www.gurobi.com/

14. https://www.ibm.com/analytics/cplex-optimizer

Appendix

A Difference Distribution Table

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

B Inequalities for Active S-Box Minimization

$$-1 * x3 - 1 * x2 + 0 * x1 - 1 * x0 + 0 * y3 + 0 * y2 + 1 * y1 + 0 * y0 \geq 2$$

$$-2 * x3 - 1 * x2 - 1 * x1 - 1 * x0 + 1 * y3 - 1 * y2 + 1 * y1 - 1 * y0 \geq 5$$

$$0 * x3 + 0 * x2 + 1 * x1 + 0 * x0 - 1 * y3 - 1 * y2 + 0 * y1 - 1 * y0 \geq 2$$

$$0 * x3 - 1 * x2 - 2 * x1 + 2 * x0 - 2 * y3 + 2 * y2 - 1 * y1 - 1 * y0 \geq 5$$

$$-2 * x3 - 2 * x2 - 1 * x1 + 3 * x0 - 1 * y3 + 3 * y2 - 2 * y1 - 1 * y0 \geq 6$$

$$0 * x3 + 1 * x2 + 1 * x1 + 1 * x0 + 1 * y3 - 2 * y2 - 1 * y1 - 2 * y0 \geq 3$$

$$0 * x3 - 1 * x2 + 1 * x1 - 1 * x0 + 0 * y3 - 1 * y2 + 1 * y1 - 1 * y0 \geq 3$$

$$1 * x3 + 1 * x2 - 1 * x1 - 2 * x0 - 2 * y3 - 2 * y2 + 1 * y1 + 2 * y0 \geq 5$$

$$0 * x3 + 1 * x2 - 2 * x1 - 2 * x0 + 2 * y3 + 1 * y2 + 1 * y1 - 1 * y0 \geq 3$$

$$-1 * x3 + 1 * x2 - 2 * x1 + 1 * x0 + 3 * y3 + 1 * y2 - 1 * y1 + 1 * y0 \geq 1$$

$$-2 * x3 + 3 * x2 - 1 * x1 - 2 * x0 - 1 * y3 - 1 * y2 - 2 * y1 + 3 * y0 \geq 6$$

$$0 * x3 - 2 * x2 - 2 * x1 + 1 * x0 + 2 * y3 - 1 * y2 + 1 * y1 + 1 * y0 \geq 3$$

$$3 * x3 + 3 * x2 + 1 * x1 + 2 * x0 - 2 * y3 + 2 * y2 - 2 * y1 + 1 * y0 \geq 0$$

$$3 * x3 - 2 * x2 + 2 * x1 + 1 * x0 - 1 * y3 - 2 * y2 - 2 * y1 + 1 * y0 \geq 4$$

$$1 * x3 - 2 * x2 - 1 * x1 + 1 * x0 - 2 * y3 + 2 * y2 + 1 * y1 - 2 * y0 \geq 5$$

$$1 * x3 + 2 * x2 + 1 * x1 + 2 * x0 + 0 * y3 - 1 * y2 + 0 * y1 - 1 * y0 \geq 0$$

$$1 * x3 - 2 * x2 - 1 * x1 - 2 * x0 + 2 * y3 + 3 * y2 + 1 * y1 + 3 * y0 \geq 1$$

$$3 * x3 + 1 * x2 + 2 * x1 - 2 * x0 - 1 * y3 + 1 * y2 - 2 * y1 - 2 * y0 \geq 4$$

$$-2 * x3 - 1 * x2 + 1 * x1 - 1 * x0 + 3 * y3 + 2 * y2 + 3 * y1 + 2 * y0 \geq 0$$

$$-1 * x3 + 2 * x2 - 1 * x1 + 2 * x0 + 0 * y3 + 1 * y2 + 2 * y1 + 1 * y0 \geq 0$$

$$1 * x3 - 1 * x2 - 1 * x1 - 1 * x0 + 0 * y3 - 1 * y2 - 1 * y1 - 1 * y0 \geq 5$$

C Inequalities for Differential Probability Minimization

$$0*x3+0*x2+0*x1+0*x0+0*y3+0*y2+0*y1+0*y0-1*p0-1*p1 \geq 1$$

$$0*x3-1*x2+0*x1-1*x0+0*y3-1*y2+0*y1-1*y0+4*p0+3*p1 \geq 0$$

$$0*x3+0*x2+0*x1+0*x0+0*y3+1*y2-1*y1+1*y0+1*p0+0*p1 \geq 0$$

$$-1*x3-1*x2+1*x1+2*x0+0*y3+0*y2-1*y1-2*y0+3*p0+4*p1 \geq 0$$

$$0*x3-3*x2-2*x1-3*x0+0*y3+1*y2+2*y1+1*y0+6*p0+5*p1 \geq 0$$

$$0*x3+2*x2-2*x1-2*x0-3*y3-1*y2-1*y1+2*y0+6*p0+7*p1 \geq 0$$

$$7*x3+4*x2+2*x1-2*x0-1*y3+4*y2-5*y1-8*y0+7*p0+10*p1 \geq 0$$

$$-4*x3+3*x2-1*x1-2*x0-1*y3-3*y2-2*y1+3*y0+8*p0+10*p1 \geq 0$$

$$1*x3+5*x2+2*x1+0*x0+2*y3-1*y2-2*y1-4*y0+2*p0+5*p1 \geq 0$$

$$0*x3+1*x2-3*x1+2*x0+1*y3+0*y2-1*y1+2*y0+3*p0+1*p1 \geq 0$$

$$-4*x3-2*x2+1*x1-2*x0+2*y3+1*y2+5*y1+1*y0+1*p0+4*p1 \geq 0$$

$$0*x3+2*x2+3*x1-1*x0-2*y3-1*y2+0*y1-1*y0+1*p0+4*p1 \geq 0$$

$$0*x3+1*x2-1*x1+1*x0+1*y3-1*y2+1*y1-1*y0+3*p0+1*p1 \geq 0$$

$$7*x3-2*x2+2*x1+4*x0-1*y3-8*y2-5*y1+4*y0+7*p0+10*p1 \geq 0$$

$$2*x3+1*x2+5*x1+1*x0-4*y3-2*y2+1*y1-2*y0+1*p0+4*p1 \geq 0$$

$$1*x3+2*x2+0*x1+2*x0+1*y3+2*y2+0*y1+2*y0-2*p0-3*p1 \geq 0$$

$$-2*x3+2*x2-4*x1-4*x0+5*y3+2*y2+1*y1-1*y0+5*p0+8*p1 \geq 0$$

$$0*x3+1*x2-3*x1+2*x0-1*y3+2*y2-1*y1-1*y0+5*p0+3*p1 \geq 0$$

$$-2*x3-4*x2-1*x1+2*x0-1*y3+2*y2+3*y1-1*y0+3*p0+8*p1 \geq 0$$

$$2*x3-4*x2-2*x1-1*x0+1*y3-1*y2-2*y1+2*y0+6*p0+10*p1 \geq 0$$