Linear codes for SSS-based polynomial masking

The SSS-based masking is a special case of GCM (Generalized Code-based masking)

$n=5$ shares, $t=2$, $\ell=4$ bits: (5,2)-SSS (Shamir's Secret Sharing)

Parameters:

- $Z=(X+Y_1\alpha_1+Y_2\alpha_1^2, X+Y_1\alpha_2+Y_2\alpha_2^2, X+Y_1\alpha_3+Y_2\alpha_3^2, X+Y_1\alpha_4+Y_2\alpha_4^2, X+Y_1\alpha_5+Y_2\alpha_5^2,)=X\mathbf{G}+Y\mathbf{H}$ where $X, Y=(Y_1,Y_2)$ and Z are the sensitive variable, a mask and the protected variable, respectively, where α_i for $1\le i\le 3$ are three public points in SSS-scheme
- $\mathbf{G}=[1,1,1,1,1]$ and $\mathbf{H}=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2\end{pmatrix}$ are two generator matrices of codes $\mathcal{C}$ and $\mathcal{D}$, resp.
- $\alpha_i\in\mathbb{F}_{2^\ell}\backslash\{0\}$ and $\alpha_1\neq\alpha_2\neq\alpha_3\neq\alpha_4\neq\alpha_5$, thus there are $\binom{15}{5}$=3003 linear codes for (5,2)-SSS
- Each nonzero element over $\mathbb{F}_{2^\ell}$ can be denoted as α^i where $i\in\{0,1,\ldots,14\}$, the corresponding irreducible polynomial is $g(\alpha)=\alpha^4+\alpha+1$
- Due to equivalence of linear codes, we simplify the enumeration by choosing $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(\alpha^i,\alpha^j,\alpha^k,\alpha^l,\alpha^r)$ where $i=0$ and $0<j<k<l<r$. Therefore, we get 1001 linear codes

In [1]:
```python
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
import re
import pandas as pd # Pandas for tables
from IPython.display import Latex
from IPython.display import HTML
```

In [2]:
```python
def read_log(file_name):

    pow_ind = []
    dim_all = []
    d_orig_w = []
    d_dual_w = []
    d_dual_b = []
    with open(file_name, 'r') as fp:
        wd = fp.read().split("\n")[:]
        len_all = 0
        for i in range(len(wd)):
            if wd[i].startswith("j, k, l, r ="):
                pow_ind.append([int(i) for i in re.findall(r"\d+", wd[i])])
                len_all = len_all + 1
            elif wd[i].startswith("Dimension:"):
                dim_all.append([int(i) for i in re.findall(r"\d+", wd[i])])
            elif wd[i].startswith("WD orig D (word):"):
                d_orig_w.append([int(i) for i in re.findall(r"\d+", wd[i])])
            elif wd[i].startswith("WD dual D (word):"):
                d_dual_w.append([int(i) for i in re.findall(r"\d+", wd[i])])
            elif wd[i].startswith("WD dual D  (bit):"):
                d_dual_b.append([int(i) for i in re.findall(r"\d+", wd[i]+wd[i+1])])
            else:
                continue

    return pow_ind, d_dual_b
```

1. Loading all weight enumerators

In [3]:
```python
pow_ind, d_dual_b = read_log("./magma_paper/gen_codes_sss_5_2_4b.log") # indices and Weight distributions

print(len(pow_ind)) # 91 entries: 771 for (5,2)-SSS
#print(len(d_dual_b))
```

```
1001
```

1.1 Generating values

In [4]:
```python
alpha_all = np.array(['$\\alpha^{%d}$'%i for i in np.arange(15)])
d_all = np.zeros(len(pow_ind))
B_all = np.zeros(len(pow_ind))
alpha_2 = np.zeros(len(pow_ind), dtype=int)
alpha_3 = np.zeros(len(pow_ind), dtype=int)
alpha_4 = np.zeros(len(pow_ind), dtype=int)
alpha_5 = np.zeros(len(pow_ind), dtype=int)
for i in range(len(pow_ind)):
    d_all[i] = d_dual_b[i][2]
    B_all[i] = d_dual_b[i][3]
    alpha_2[i] = pow_ind[i][0]
    alpha_3[i] = pow_ind[i][1]
    alpha_4[i] = pow_ind[i][2]
    alpha_5[i] = pow_ind[i][3]
```

1.2 Defining styles of dataframe

In [5]:
```python
# Set properties for th, td and caption elements in dataframe
th_props = [('font-size', '14px'), ('text-align', 'left'), ('font-weight', 'bold'), ('background-color', '#E0E0E0')]
td_props = [('font-size', '13px'), ('text-align', 'left'), ('min-width', '60px')]
cp_props = [('font-size', '16px'), ('text-align', 'center')]
# Set table styles
styles = [dict(selector="th", props=th_props), dict(selector="td", props=td_props), dict(selector="caption", props=cp_props)]
cm_1 = sns.light_palette("red", as_cmap=True)
cm_2 = sns.light_palette("purple", as_cmap=True, reverse=True)
```

We only show the first 500 codes because of the limit on file size..

In [6]:
```python
c_max = 500
df = pd.DataFrame({'$\\alpha_2$': alpha_all[alpha_2[:c_max]], '$\\alpha_3$': alpha_all[alpha_3[:c_max]], '$\\alpha_4$': alpha_all[alpha_4[:c_max]]
                   '$\\alpha_5$': alpha_all[alpha_5[:c_max]], '$d_{\mathcal{D}}^\perp$': d_all[:c_max],
                   '$B_{d_{\mathcal{D}}^\perp}$': B_all[:c_max], 'Weight Enumerators* (the first 24 elements)': d_dual_b[:c_max]})

pd.set_option('display.max_colwidth', 1000)
pd.set_option('display.width', 800)
(df.style
   .background_gradient(cmap=cm_1, subset=['$d_{\mathcal{D}}^\perp$','$B_{d_{\mathcal{D}}^\perp}$' ])
   .background_gradient(cmap=cm_2, subset=['$B_{d_{\mathcal{D}}^\perp}$' ])
   .set_caption('Tab. I All linear codes for (5,2)-SSS-based masking with $n=5$ shares over $\mathbb{F}_{2^4}$.')
   .set_table_styles(styles))
```

Out[6]:

Tab. I All linear codes for (5,2)-SSS-based masking with $n=5$ shares over $\mathbb{F}_{2^4}$.

	α_2	α_3	α_4	α_5	$d_{\mathcal{D}}^{\perp}$	$B_{d_{\mathcal{D}}^{\perp}}$	Weight Enumerators* (the first 24 elements)
0	α^1	α^2	α^3	α^4	3	4	[0, 1, 3, 4, 4, 14, 5, 63, 6, 156, 7, 302, 8, 500, 9, 645, 10, 712, 11, 680, 1, 2, 3, 5]
1	α^1	α^2	α^3	α^5	3	4	[0, 1, 3, 4, 4, 13, 5, 67, 6, 165, 7, 288, 8, 477, 9, 663, 10, 735, 11, 668, 1, 2, 3, 6]
2	α^1	α^2	α^3	α^6	3	6	[0, 1, 3, 6, 4, 14, 5, 61, 6, 157, 7, 288, 8, 502, 9, 683, 10, 695, 11, 638, 1, 2, 3, 7]
3	α^1	α^2	α^3	α^7	3	3	[0, 1, 3, 3, 4, 16, 5, 60, 6, 155, 7, 315, 8, 490, 9, 644, 10, 723, 11, 649, 1, 2, 3, 8]
4	α^1	α^2	α^3	α^8	3	6	[0, 1, 3, 6, 4, 12, 5, 61, 6, 166, 7, 288, 8, 486, 9, 683, 10, 710, 11, 638, 1, 2, 3, 9]
5	α^1	α^2	α^3	α^9	3	4	[0, 1, 3, 4, 4, 15, 5, 64, 6, 150, 7, 296, 8, 515, 9, 660, 10, 692, 11, 660, 1, 2, 3, 10]
6	α^1	α^2	α^3	α^{10}	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 1, 2, 3, 11]
7	α^1	α^2	α^3	α^{11}	3	1	[0, 1, 3, 1, 4, 17, 5, 70, 6, 148, 7, 301, 8, 503, 9, 642, 10, 720, 11, 667, 1, 2, 3, 12]
8	α^1	α^2	α^3	α^{12}	3	1	[0, 1, 3, 1, 4, 17, 5, 67, 6, 152, 7, 305, 8, 494, 9, 651, 10, 720, 11, 651, 1, 2, 3, 13]
9	α^1	α^2	α^3	α^{13}	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 1, 2, 3, 14]
10	α^1	α^2	α^3	α^{14}	3	4	[0, 1, 3, 4, 4, 14, 5, 63, 6, 156, 7, 302, 8, 500, 9, 645, 10, 712, 11, 680, 1, 2, 4, 5]
11	α^1	α^2	α^4	α^5	3	8	[0, 1, 3, 8, 4, 13, 5, 49, 6, 165, 7, 316, 8, 477, 9, 653, 10, 735, 11, 648, 1, 2, 4, 6]
12	α^1	α^2	α^4	α^6	3	7	[0, 1, 3, 7, 4, 14, 5, 52, 6, 155, 7, 311, 8, 504, 9, 660, 10, 707, 11, 645, 1, 2, 4, 7]
13	α^1	α^2	α^4	α^7	3	6	[0, 1, 3, 6, 4, 10, 5, 58, 6, 178, 7, 302, 8, 456, 9, 658, 10, 750, 11, 658, 1, 2, 4, 8]
14	α^1	α^2	α^4	α^8	3	9	[0, 1, 3, 9, 4, 12, 5, 46, 6, 166, 7, 313, 8, 480, 9, 670, 10, 732, 11, 635, 1, 2, 4, 9]
15	α^1	α^2	α^4	α^9	3	4	[0, 1, 3, 4, 4, 11, 5, 62, 6, 170, 7, 304, 8, 475, 9, 650, 10, 735, 11, 660, 1, 2, 4, 10]
16	α^1	α^2	α^4	α^{10}	3	8	[0, 1, 3, 8, 4, 13, 5, 52, 6, 162, 7, 300, 8, 485, 9, 680, 10, 732, 11, 640, 1, 2, 4, 11]
17	α^1	α^2	α^4	α^{11}	3	5	[0, 1, 3, 5, 4, 13, 5, 60, 6, 160, 7, 301, 8, 495, 9, 660, 10, 712, 11, 655, 1, 2, 4, 12]
18	α^1	α^2	α^4	α^{12}	3	5	[0, 1, 3, 5, 4, 14, 5, 58, 6, 160, 7, 303, 8, 488, 9, 672, 10, 720, 11, 627, 1, 2, 4, 13]
19	α^1	α^2	α^4	α^{13}	3	5	[0, 1, 3, 5, 4, 14, 5, 58, 6, 158, 7, 309, 8, 490, 9, 650, 10, 732, 11, 655, 1, 2, 4, 14]
20	α^1	α^2	α^4	α^{14}	3	4	[0, 1, 3, 4, 4, 13, 5, 67, 6, 165, 7, 288, 8, 477, 9, 663, 10, 735, 11, 668, 1, 2, 5, 6]
21	α^1	α^2	α^5	α^6	3	6	[0, 1, 3, 6, 4, 13, 5, 59, 6, 165, 7, 288, 8, 486, 9, 683, 10, 735, 11, 658, 1, 2, 5, 7]
22	α^1	α^2	α^5	α^7	3	7	[0, 1, 3, 7, 4, 14, 5, 56, 6, 162, 7, 299, 8, 478, 9, 668, 10, 740, 11, 653, 1, 2, 5, 8]
23	α^1	α^2	α^5	α^8	3	8	[0, 1, 3, 8, 4, 12, 5, 53, 6, 172, 7, 304, 8, 464, 9, 661, 10, 738, 11, 656, 1, 2, 5, 9]
24	α^1	α^2	α^5	α^9	3	5	[0, 1, 3, 5, 4, 16, 5, 62, 6, 154, 7, 297, 8, 488, 9, 658, 10, 740, 11, 663, 1, 2, 5, 10]
25	α^1	α^2	α^5	α^{10}	3	8	[0, 1, 3, 8, 4, 11, 5, 50, 6, 170, 7, 308, 8, 475, 9, 670, 10, 732, 11, 640, 1, 2, 5, 11]
26	α^1	α^2	α^5	α^{11}	3	5	[0, 1, 3, 5, 4, 15, 5, 61, 6, 159, 7, 301, 8, 477, 9, 670, 10, 733, 11, 663, 1, 2, 5, 12]
27	α^1	α^2	α^5	α^{12}	3	4	[0, 1, 3, 4, 4, 14, 5, 60, 6, 164, 7, 308, 8, 468, 9, 652, 10, 760, 11, 652, 1, 2, 5, 13]
28	α^1	α^2	α^5	α^{13}	3	5	[0, 1, 3, 5, 4, 15, 5, 56, 6, 155, 7, 311, 8, 497, 9, 662, 10, 715, 11, 627, 1, 2, 5, 14]
29	α^1	α^2	α^5	α^{14}	3	6	[0, 1, 3, 6, 4, 14, 5, 61, 6, 157, 7, 288, 8, 502, 9, 683, 10, 695, 11, 638, 1, 2, 6, 7]
30	α^1	α^2	α^6	α^7	3	4	[0, 1, 3, 4, 4, 11, 5, 64, 6, 164, 7, 296, 8, 500, 9, 660, 10, 696, 11, 660, 1, 2, 6, 8]
31	α^1	α^2	α^6	α^8	3	7	[0, 1, 3, 7, 4, 14, 5, 55, 6, 162, 7, 305, 8, 478, 9, 670, 10, 740, 11, 673, 1, 2, 6, 9]
32	α^1	α^2	α^6	α^9	3	2	[0, 1, 3, 2, 4, 17, 5, 67, 6, 154, 7, 296, 8, 481, 9, 669, 10, 748, 11, 634, 1, 2, 6, 10]
33	α^1	α^2	α^6	α^{10}	3	2	[0, 1, 3, 2, 4, 17, 5, 66, 6, 150, 7, 302, 8, 501, 9, 654, 10, 708, 11, 654, 1, 2, 6, 11]
34	α^1	α^2	α^6	α^{11}	3	7	[0, 1, 3, 7, 4, 15, 5, 54, 6, 151, 7, 301, 8, 509, 9, 680, 10, 707, 11, 625, 1, 2, 6, 12]
35	α^1	α^2	α^6	α^{12}	3	2	[0, 1, 3, 2, 4, 22, 5, 53, 6, 147, 7, 330, 8, 488, 9, 645, 10, 723, 11, 638, 1, 2, 6, 13]
36	α^1	α^2	α^6	α^{13}	3	6	[0, 1, 3, 6, 4, 12, 5, 58, 6, 164, 7, 298, 8, 499, 9, 670, 10, 712, 11, 650, 1, 2, 6, 14]
37	α^1	α^2	α^6	α^{14}	3	3	[0, 1, 3, 3, 4, 16, 5, 60, 6, 155, 7, 315, 8, 490, 9, 644, 10, 723, 11, 649, 1, 2, 7, 8]
38	α^1	α^2	α^7	α^8	3	6	[0, 1, 3, 6, 4, 10, 5, 59, 6, 173, 7, 292, 8, 474, 9, 685, 10, 727, 11, 630, 1, 2, 7, 9]
39	α^1	α^2	α^7	α^9	3	6	[0, 1, 3, 6, 4, 12, 5, 57, 6, 166, 7, 302, 8, 480, 9, 665, 10, 732, 11, 650, 1, 2, 7, 10]
40	α^1	α^2	α^7	α^{10}	3	2	[0, 1, 3, 2, 4, 14, 5, 69, 6, 161, 7, 292, 8, 482, 9, 667, 10, 735, 11, 642, 1, 2, 7, 11]
41	α^1	α^2	α^7	α^{11}	3	3	[0, 1, 3, 3, 4, 17, 5, 59, 6, 155, 7, 315, 8, 483, 9, 651, 10, 731, 11, 671, 1, 2, 7, 12]
42	α^1	α^2	α^7	α^{12}	3	6	[0, 1, 3, 6, 4, 13, 5, 56, 6, 160, 7, 308, 8, 495, 9, 650, 10, 712, 11, 670, 1, 2, 7, 13]
43	α^1	α^2	α^7	α^{13}	3	2	[0, 1, 3, 2, 4, 16, 5, 63, 6, 154, 7, 314, 8, 496, 9, 639, 10, 708, 11, 654, 1, 2, 7, 14]
44	α^1	α^2	α^7	α^{14}	3	6	[0, 1, 3, 6, 4, 12, 5, 61, 6, 166, 7, 288, 8, 486, 9, 683, 10, 710, 11, 638, 1, 2, 8, 9]
45	α^1	α^2	α^8	α^9	3	4	[0, 1, 3, 4, 4, 15, 5, 67, 6, 154, 7, 288, 8, 501, 9, 663, 10, 710, 11, 668, 1, 2, 8, 10]
46	α^1	α^2	α^8	α^{10}	3	8	[0, 1, 3, 8, 4, 11, 5, 50, 6, 170, 7, 308, 8, 475, 9, 670, 10, 732, 11, 640, 1, 2, 8, 11]
47	α^1	α^2	α^8	α^{11}	3	6	[0, 1, 3, 6, 4, 17, 5, 54, 6, 152, 7, 316, 8, 491, 9, 640, 10, 728, 11, 670, 1, 2, 8, 12]
48	α^1	α^2	α^8	α^{12}	3	4	[0, 1, 3, 4, 4, 12, 5, 61, 6, 163, 7, 308, 8, 494, 9, 645, 10, 707, 11, 660, 1, 2, 8, 13]
49	α^1	α^2	α^8	α^{13}	3	4	[0, 1, 3, 4, 4, 11, 5, 62, 6, 167, 7, 304, 8, 489, 9, 650, 10, 707, 11, 660, 1, 2, 8, 14]
50	α^1	α^2	α^8	α^{14}	3	4	[0, 1, 3, 4, 4, 15, 5, 64, 6, 150, 7, 296, 8, 515, 9, 660, 10, 692, 11, 660, 1, 2, 9, 10]
51	α^1	α^2	α^9	α^{10}	3	2	[0, 1, 3, 2, 4, 17, 5, 70, 6, 148, 7, 288, 8, 503, 9, 672, 10, 720, 11, 642, 1, 2, 9, 11]
52	α^1	α^2	α^9	α^{11}	3	5	[0, 1, 3, 5, 4, 14, 5, 62, 6, 159, 7, 297, 8, 492, 9, 658, 10, 715, 11, 663, 1, 2, 9, 12]
53	α^1	α^2	α^9	α^{12}	3	1	[0, 1, 3, 1, 4, 22, 5, 57, 6, 162, 7, 303, 8, 454, 9, 699, 10, 740, 11, 615, 1, 2, 9, 13]
54	α^1	α^2	α^9	α^{13}	3	1	[0, 1, 3, 1, 4, 15, 5, 71, 6, 156, 7, 293, 8, 496, 9, 659, 10, 712, 11, 659, 1, 2, 9, 14]
55	α^1	α^2	α^9	α^{14}	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 1, 2, 10, 11]
56	α^1	α^2	α^{10}	α^{11}	3	3	[0, 1, 3, 3, 4, 15, 5, 68, 6, 149, 7, 291, 8, 519, 9, 660, 10, 687, 11, 665, 1, 2, 10, 12]
57	α^1	α^2	α^{10}	α^{12}	4	17	[0, 1, 4, 17, 5, 70, 6, 151, 7, 308, 8, 495, 9, 634, 10, 723, 11, 664, 12, 491, 1, 2, 10, 13]
58	α^1	α^2	α^{10}	α^{13}	3	1	[0, 1, 3, 1, 4, 17, 5, 71, 6, 153, 7, 291, 8, 485, 9, 669, 10, 743, 11, 639, 1, 2, 10, 14]
59	α^1	α^2	α^{10}	α^{14}	3	1	[0, 1, 3, 1, 4, 17, 5, 70, 6, 148, 7, 301, 8, 503, 9, 642, 10, 720, 11, 667, 1, 2, 11, 12]
60	α^1	α^2	α^{11}	α^{12}	3	7	[0, 1, 3, 7, 4, 15, 5, 52, 6, 152, 7, 311, 8, 505, 9, 660, 10, 712, 11, 645, 1, 2, 11, 13]
61	α^1	α^2	α^{11}	α^{13}	3	1	[0, 1, 3, 1, 4, 20, 5, 64, 6, 140, 7, 317, 8, 512, 9, 636, 10, 706, 11, 651, 1, 2, 11, 14]
62	α^1	α^2	α^{11}	α^{14}	3	1	[0, 1, 3, 1, 4, 17, 5, 67, 6, 152, 7, 305, 8, 494, 9, 651, 10, 720, 11, 651, 1, 2, 12, 13]
63	α^1	α^2	α^{12}	α^{13}	3	4	[0, 1, 3, 4, 4, 11, 5, 62, 6, 167, 7, 304, 8, 489, 9, 650, 10, 707, 11, 660, 1, 2, 12, 14]
64	α^1	α^2	α^{12}	α^{14}	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 1, 2, 13, 14]
65	α^1	α^2	α^{13}	α^{14}	3	4	[0, 1, 3, 4, 4, 14, 5, 63, 6, 156, 7, 302, 8, 500, 9, 645, 10, 712, 11, 680, 1, 3, 4, 5]
66	α^1	α^3	α^4	α^5	3	4	[0, 1, 3, 4, 4, 11, 5, 62, 6, 167, 7, 304, 8, 489, 9, 650, 10, 707, 11, 660, 1, 3, 4, 6]
67	α^1	α^3	α^4	α^6	3	7	[0, 1, 3, 7, 4, 14, 5, 55, 6, 157, 7, 303, 8, 502, 9, 663, 10, 695, 11, 673, 1, 3, 4, 7]
68	α^1	α^3	α^4	α^7	3	9	[0, 1, 3, 9, 4, 15, 5, 47, 6, 154, 7, 309, 8, 495, 9, 675, 10, 732, 11, 635, 1, 3, 4, 8]
69	α^1	α^3	α^4	α^8	3	5	[0, 1, 3, 5, 4, 10, 5, 58, 6, 174, 7, 309, 8, 470, 9, 650, 10, 740, 11, 660, 1, 3, 4, 9]
70	α^1	α^3	α^4	α^9	3	10	[0, 1, 3, 10, 4, 15, 5, 40, 6, 154, 7, 326, 8, 495, 9, 660, 10, 732, 11, 630, 1, 3, 4, 10]
71	α^1	α^3	α^4	α^{10}	3	4	[0, 1, 3, 4, 4, 12, 5, 59, 6, 167, 7, 312, 8, 482, 9, 647, 10, 715, 11, 652, 1, 3, 4, 11]
72	α^1	α^3	α^4	α^{11}	3	4	[0, 1, 3, 4, 4, 11, 5, 63, 6, 166, 7, 300, 8, 493, 9, 655, 10, 702, 11, 660, 1, 3, 4, 12]
73	α^1	α^3	α^4	α^{12}	3	6	[0, 1, 3, 6, 4, 14, 5, 53, 6, 156, 7, 320, 8, 500, 9, 635, 10, 712, 11, 670, 1, 3, 4, 13]
74	α^1	α^3	α^4	α^{13}	3	6	[0, 1, 3, 6, 4, 16, 5, 61, 6, 153, 7, 310, 8, 500, 9, 635, 10, 703, 11, 680, 1, 3, 4, 14]
75	α^1	α^3	α^4	α^{14}	3	8	[0, 1, 3, 8, 4, 13, 5, 49, 6, 165, 7, 316, 8, 477, 9, 653, 10, 735, 11, 648, 1, 3, 5, 6]
76	α^1	α^3	α^5	α^6	3	2	[0, 1, 3, 2, 4, 17, 5, 66, 6, 150, 7, 302, 8, 501, 9, 647, 10, 730, 11, 662, 1, 3, 5, 7]
77	α^1	α^3	α^5	α^7	3	2	[0, 1, 3, 2, 4, 17, 5, 64, 6, 152, 7, 312, 8, 491, 9, 634, 10, 728, 11, 674, 1, 3, 5, 8]
78	α^1	α^3	α^5	α^8	4	17	[0, 1, 4, 17, 5, 68, 6, 164, 7, 294, 8, 471, 9, 678, 10, 720, 11, 636, 12, 515, 1, 3, 5, 9]
79	α^1	α^3	α^5	α^9	3	4	[0, 1, 3, 4, 4, 14, 5, 61, 6, 153, 7, 310, 8, 514, 9, 635, 10, 687, 11, 680, 1, 3, 5, 10]
80	α^1	α^3	α^5	α^{10}	3	4	[0, 1, 3, 4, 4, 11, 5, 63, 6, 170, 7, 298, 8, 475, 9, 665, 10, 732, 11, 640, 1, 3, 5, 11]
81	α^1	α^3	α^5	α^{11}	3	4	[0, 1, 3, 4, 4, 12, 5, 62, 6, 158, 7, 304, 8, 505, 9, 650, 10, 692, 11, 660, 1, 3, 5, 12]
82	α^1	α^3	α^5	α^{12}	3	1	[0, 1, 3, 1, 4, 16, 5, 69, 6, 152, 7, 305, 8, 498, 9, 637, 10, 720, 11, 667, 1, 3, 5, 13]
83	α^1	α^3	α^5	α^{13}	3	1	[0, 1, 3, 1, 4, 13, 5, 71, 6, 168, 7, 293, 8, 466, 9, 659, 10, 752, 11, 659, 1, 3, 5, 14]
84	α^1	α^3	α^5	α^{14}	3	8	[0, 1, 3, 8, 4, 14, 5, 51, 6, 153, 7, 311, 8, 504, 9, 660, 10, 707, 11, 645, 1, 3, 6, 7]
85	α^1	α^3	α^6	α^7	3	3	[0, 1, 3, 3, 4, 15, 5, 65, 6, 154, 7, 299, 8, 503, 9, 657, 10, 700, 11, 657, 1, 3, 6, 8]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
446	α^2	α^6	α^{11}	α^{14}	3	2	[0, 1, 3, 2, 4, 16, 5, 63, 6, 155, 7, 314, 8, 490, 9, 639, 10, 723, 11, 654, 2, 6, 12, 13]
447	α^2	α^6	α^{12}	α^{13}	3	4	[0, 1, 3, 4, 4, 14, 5, 61, 6, 153, 7, 310, 8, 514, 9, 635, 10, 687, 11, 680, 2, 6, 12, 14]
448	α^2	α^6	α^{12}	α^{14}	3	1	[0, 1, 3, 1, 4, 19, 5, 63, 6, 149, 7, 323, 8, 483, 9, 621, 10, 751, 11, 671, 2, 6, 13, 14]
449	α^2	α^6	α^{13}	α^{14}	3	9	[0, 1, 3, 9, 4, 12, 5, 46, 6, 166, 7, 313, 8, 480, 9, 670, 10, 732, 11, 635, 2, 7, 8, 9]
450	α^2	α^7	α^8	α^9	3	8	[0, 1, 3, 8, 4, 11, 5, 50, 6, 170, 7, 308, 8, 475, 9, 670, 10, 732, 11, 640, 2, 7, 8, 10]
451	α^2	α^7	α^8	α^{10}	3	4	[0, 1, 3, 4, 4, 10, 5, 63, 6, 172, 7, 298, 8, 480, 9, 665, 10, 712, 11, 640, 2, 7, 8, 11]
452	α^2	α^7	α^8	α^{11}	3	10	[0, 1, 3, 10, 4, 18, 5, 49, 6, 152, 7, 302, 8, 482, 9, 669, 10, 746, 11, 654, 2, 7, 8, 12]
453	α^2	α^7	α^8	α^{12}	3	8	[0, 1, 3, 8, 4, 13, 5, 50, 6, 162, 7, 308, 8, 485, 9, 670, 10, 732, 11, 640, 2, 7, 8, 13]
454	α^2	α^7	α^8	α^{13}	3	6	[0, 1, 3, 6, 4, 12, 5, 62, 6, 176, 7, 290, 8, 446, 9, 666, 10, 768, 11, 666, 2, 7, 8, 14]
455	α^2	α^7	α^8	α^{14}	3	4	[0, 1, 3, 4, 4, 16, 5, 64, 6, 154, 7, 296, 8, 494, 9, 660, 10, 718, 11, 660, 2, 7, 9, 10]
456	α^2	α^7	α^9	α^{10}	3	6	[0, 1, 3, 6, 4, 11, 5, 55, 6, 172, 7, 310, 8, 465, 9, 655, 10, 752, 11, 650, 2, 7, 9, 11]
457	α^2	α^7	α^9	α^{11}	3	9	[0, 1, 3, 9, 4, 15, 5, 43, 6, 154, 7, 325, 8, 495, 9, 655, 10, 732, 11, 635, 2, 7, 9, 12]
458	α^2	α^7	α^9	α^{12}	3	8	[0, 1, 3, 8, 4, 14, 5, 49, 6, 158, 7, 312, 8, 490, 9, 665, 10, 732, 11, 640, 2, 7, 9, 13]
459	α^2	α^7	α^9	α^{13}	3	5	[0, 1, 3, 5, 4, 12, 5, 58, 6, 166, 7, 309, 8, 480, 9, 650, 10, 732, 11, 660, 2, 7, 9, 14]
460	α^2	α^7	α^9	α^{14}	3	4	[0, 1, 3, 4, 4, 10, 5, 63, 6, 172, 7, 298, 8, 480, 9, 665, 10, 712, 11, 640, 2, 7, 10, 11]
461	α^2	α^7	α^{10}	α^{11}	3	1	[0, 1, 3, 1, 4, 17, 5, 66, 6, 153, 7, 309, 8, 493, 9, 646, 10, 711, 11, 651, 2, 7, 10, 12]
462	α^2	α^7	α^{10}	α^{12}	3	4	[0, 1, 3, 4, 4, 11, 5, 61, 6, 173, 7, 304, 8, 467, 9, 657, 10, 735, 11, 652, 2, 7, 10, 13]
463	α^2	α^7	α^{10}	α^{13}	3	1	[0, 1, 3, 1, 4, 16, 5, 67, 6, 158, 7, 311, 8, 476, 9, 629, 10, 748, 11, 679, 2, 7, 10, 14]
464	α^2	α^7	α^{10}	α^{14}	3	1	[0, 1, 3, 1, 4, 13, 5, 71, 6, 168, 7, 293, 8, 466, 9, 659, 10, 752, 11, 659, 2, 7, 11, 12]
465	α^2	α^7	α^{11}	α^{12}	3	11	[0, 1, 3, 11, 4, 20, 5, 44, 6, 142, 7, 307, 8, 496, 9, 676, 10, 748, 11, 641, 2, 7, 11, 13]
466	α^2	α^7	α^{11}	α^{13}	3	2	[0, 1, 3, 2, 4, 20, 5, 53, 6, 164, 7, 312, 8, 466, 9, 687, 10, 712, 11, 618, 2, 7, 11, 14]
467	α^2	α^7	α^{11}	α^{14}	3	1	[0, 1, 3, 1, 4, 19, 5, 64, 6, 148, 7, 317, 8, 489, 9, 636, 10, 736, 11, 651, 2, 7, 12, 13]
468	α^2	α^7	α^{12}	α^{13}	3	4	[0, 1, 3, 4, 4, 11, 5, 63, 6, 170, 7, 298, 8, 475, 9, 665, 10, 732, 11, 640, 2, 7, 12, 14]
469	α^2	α^7	α^{12}	α^{14}	3	4	[0, 1, 3, 4, 4, 11, 5, 62, 6, 167, 7, 304, 8, 489, 9, 650, 10, 707, 11, 660, 2, 7, 13, 14]
470	α^2	α^7	α^{13}	α^{14}	3	4	[0, 1, 3, 4, 4, 11, 5, 62, 6, 170, 7, 304, 8, 479, 9, 650, 10, 732, 11, 640, 2, 8, 9, 10]
471	α^2	α^8	α^9	α^{10}	3	6	[0, 1, 3, 6, 4, 12, 5, 57, 6, 166, 7, 302, 8, 480, 9, 665, 10, 732, 11, 650, 2, 8, 9, 11]
472	α^2	α^8	α^9	α^{11}	3	10	[0, 1, 3, 10, 4, 16, 5, 45, 6, 154, 7, 310, 8, 488, 9, 673, 10, 740, 11, 638, 2, 8, 9, 12]
473	α^2	α^8	α^9	α^{12}	3	8	[0, 1, 3, 8, 4, 13, 5, 46, 6, 162, 7, 324, 8, 485, 9, 650, 10, 732, 11, 640, 2, 8, 9, 13]
474	α^2	α^8	α^9	α^{13}	3	5	[0, 1, 3, 5, 4, 14, 5, 56, 6, 160, 7, 313, 8, 486, 9, 652, 10, 730, 11, 647, 2, 8, 9, 14]
475	α^2	α^8	α^9	α^{14}	3	6	[0, 1, 3, 6, 4, 11, 5, 55, 6, 168, 7, 310, 8, 485, 9, 655, 10, 712, 11, 650, 2, 8, 10, 11]
476	α^2	α^8	α^{10}	α^{11}	3	6	[0, 1, 3, 6, 4, 13, 5, 56, 6, 159, 7, 306, 8, 499, 9, 660, 10, 707, 11, 650, 2, 8, 10, 12]
477	α^2	α^8	α^{10}	α^{12}	3	4	[0, 1, 3, 4, 4, 13, 5, 59, 6, 162, 7, 312, 8, 491, 9, 647, 10, 710, 11, 652, 2, 8, 10, 13]
478	α^2	α^8	α^{10}	α^{13}	3	5	[0, 1, 3, 5, 4, 12, 5, 59, 6, 165, 7, 305, 8, 484, 9, 655, 10, 727, 11, 655, 2, 8, 10, 14]
479	α^2	α^8	α^{10}	α^{14}	3	4	[0, 1, 3, 4, 4, 12, 5, 62, 6, 162, 7, 304, 8, 498, 9, 650, 10, 702, 11, 660, 2, 8, 11, 12]
480	α^2	α^8	α^{11}	α^{12}	3	12	[0, 1, 3, 12, 4, 20, 5, 41, 6, 142, 7, 308, 8, 496, 9, 681, 10, 748, 11, 636, 2, 8, 11, 13]
481	α^2	α^8	α^{11}	α^{13}	3	6	[0, 1, 3, 6, 4, 16, 5, 58, 6, 152, 7, 308, 8, 476, 9, 636, 10, 748, 11, 686, 2, 8, 11, 14]
482	α^2	α^8	α^{11}	α^{14}	3	6	[0, 1, 3, 6, 4, 17, 5, 57, 6, 151, 7, 300, 8, 495, 9, 675, 10, 723, 11, 630, 2, 8, 12, 13]
483	α^2	α^8	α^{12}	α^{13}	3	4	[0, 1, 3, 4, 4, 13, 5, 62, 6, 158, 7, 304, 8, 505, 9, 650, 10, 692, 11, 660, 2, 8, 12, 14]
484	α^2	α^8	α^{12}	α^{14}	3	5	[0, 1, 3, 5, 4, 15, 5, 57, 6, 155, 7, 309, 8, 497, 9, 657, 10, 715, 11, 647, 2, 8, 13, 14]
485	α^2	α^8	α^{13}	α^{14}	3	8	[0, 1, 3, 8, 4, 13, 5, 52, 6, 162, 7, 300, 8, 485, 9, 680, 10, 732, 11, 640, 2, 9, 10, 11]
486	α^2	α^9	α^{10}	α^{11}	3	7	[0, 1, 3, 7, 4, 14, 5, 55, 6, 162, 7, 305, 8, 478, 9, 653, 10, 740, 11, 673, 2, 9, 10, 12]
487	α^2	α^9	α^{10}	α^{12}	3	2	[0, 1, 3, 2, 4, 18, 5, 57, 6, 165, 7, 312, 8, 458, 9, 675, 10, 743, 11, 618, 2, 9, 10, 13]
488	α^2	α^9	α^{10}	α^{13}	3	8	[0, 1, 3, 8, 4, 15, 5, 55, 6, 161, 7, 296, 8, 475, 9, 671, 10, 743, 11, 656, 2, 9, 10, 14]
489	α^2	α^9	α^{10}	α^{14}	3	2	[0, 1, 3, 2, 4, 18, 5, 61, 6, 161, 7, 300, 8, 470, 9, 683, 10, 735, 11, 626, 2, 9, 11, 12]
490	α^2	α^9	α^{11}	α^{12}	3	11	[0, 1, 3, 11, 4, 20, 5, 48, 6, 146, 7, 295, 8, 484, 9, 684, 10, 756, 11, 649, 2, 9, 11, 13]
491	α^2	α^9	α^{11}	α^{13}	3	6	[0, 1, 3, 6, 4, 14, 5, 50, 6, 158, 7, 326, 8, 496, 9, 642, 10, 710, 11, 642, 2, 9, 11, 14]
492	α^2	α^9	α^{11}	α^{14}	3	5	[0, 1, 3, 5, 4, 14, 5, 63, 6, 157, 7, 293, 8, 502, 9, 663, 10, 695, 11, 663, 2, 9, 12, 13]
493	α^2	α^9	α^{12}	α^{13}	3	1	[0, 1, 3, 1, 4, 16, 5, 69, 6, 152, 7, 305, 8, 498, 9, 637, 10, 720, 11, 667, 2, 9, 12, 14]
494	α^2	α^9	α^{12}	α^{14}	4	23	[0, 1, 4, 23, 5, 56, 6, 154, 7, 320, 8, 479, 9, 664, 10, 700, 11, 640, 12, 537, 2, 9, 13, 14]
495	α^2	α^9	α^{13}	α^{14}	3	5	[0, 1, 3, 5, 4, 13, 5, 60, 6, 160, 7, 301, 8, 495, 9, 660, 10, 712, 11, 655, 2, 10, 11, 12]
496	α^2	α^{10}	α^{11}	α^{12}	3	7	[0, 1, 3, 7, 4, 14, 5, 56, 6, 162, 7, 299, 8, 478, 9, 668, 10, 740, 11, 653, 2, 10, 11, 13]
497	α^2	α^{10}	α^{11}	α^{13}	3	2	[0, 1, 3, 2, 4, 17, 5, 64, 6, 152, 7, 312, 8, 491, 9, 634, 10, 728, 11, 674, 2, 10, 11, 14]
498	α^2	α^{10}	α^{11}	α^{14}	3	5	[0, 1, 3, 5, 4, 11, 5, 61, 6, 173, 7, 303, 8, 467, 9, 643, 10, 735, 11, 683, 2, 10, 12, 13]
499	α^2	α^{10}	α^{12}	α^{13}	3	1	[0, 1, 3, 1, 4, 13, 5, 71, 6, 168, 7, 293, 8, 466, 9, 659, 10, 752, 11, 659, 2, 10, 12, 14]

2. Optimal linear codes for (5,2)-SSS-based masking

2.1 Linear codes with $d_{\mathcal{D}}^{\perp}=4$

We focus on the the linear codes with greater $d_{\mathcal{D}}^{\perp}$, which are better in the sense of side-channel resistance (from our paper).

In [7]:
```python
# Finding the indices of d_C=4
d_index = []
d_index_alpha_2 = []
d_index_alpha_3 = []
d_index_alpha_4 = []
d_index_alpha_5 = []
d_D_perp = 4
for i in range(len(d_dual_b)):
    if d_dual_b[i][2] == d_D_perp:
        d_index.append(i)
        d_index_alpha_2.append(pow_ind[i][0])
        d_index_alpha_3.append(pow_ind[i][1])
        d_index_alpha_4.append(pow_ind[i][2])
        d_index_alpha_5.append(pow_ind[i][3])

d_index = np.array(d_index)
d_index_alpha_2 = np.array(d_index_alpha_2)
d_index_alpha_3 = np.array(d_index_alpha_3)
d_index_alpha_4 = np.array(d_index_alpha_4)
d_index_alpha_5 = np.array(d_index_alpha_5)
```

In [8]:
```python
print(len(d_index))
print(d_index)
```

```
51
[  6   9  55  57  64  78 113 116 181 233 242 243 265 272 284 286 302 303
 328 342 364 386 391 419 437 494 500 513 541 543 552 556 566 574 594 597
 601 602 662 740 748 791 892 917 919 937 959 965 979 981 999]
```

In [20]:
```python
def highlight(s, threshold, column):
    is_min = pd.Series(data=False, index=s.index)
    is_min[column] = (s.loc[column] <= threshold)
    return ['background-color: gold' if is_min.any() else '' for v in is_min]
```

In [21]:
```python
df_4 = pd.DataFrame({'$\\alpha_2$': np.array(alpha_all)[d_index_alpha_2], '$\\alpha_3$': np.array(alpha_all)[d_index_alpha_3],
                     '$\\alpha_4$': np.array(alpha_all)[d_index_alpha_4], '$\\alpha_5$': np.array(alpha_all)[d_index_alpha_5],
                     '$d_{\mathcal{D}}^\perp$': d_all[d_index], '$B_{d_{\mathcal{D}}^\perp}$': B_all[d_index], 'Weight Enumerators* (the first 24
df_4 = df_4.sort_values(by=['$B_{d_{\mathcal{D}}^\perp}$'], ascending=True)

(df_4.style
    .apply(highlight, threshold=17, column=['$B_{d_{\mathcal{D}}^\perp}$'], axis=1)
    .background_gradient(cmap=cm_2, subset=['$B_{d_{\mathcal{D}}^\perp}$' ])
    .set_caption('Tab. II Linear codes for (5,2)-SSS-based masking with $d_{\mathcal{D}}^\perp=4$.')
    .set_table_styles(styles))
```

Out[21]:

Tab. II Linear codes for (5,2)-SSS-based masking with $d_{\mathcal{D}}^{\perp}=4$.

	α_2	α_3	α_4	α_5	$d_{\mathcal{D}}^{\perp}$	$B_{d_{\mathcal{D}}^{\perp}}$	Weight Enumerators* (the first 24 elements)
38	α^3	α^{10}	α^{11}	α^{13}	4	17	[0, 1, 4, 17, 5, 68, 6, 164, 7, 294, 8, 471, 9, 678, 10, 720, 11, 636, 12, 515, 3, 10, 11, 14]
27	α^3	α^4	α^5	α^{13}	4	17	[0, 1, 4, 17, 5, 70, 6, 151, 7, 308, 8, 495, 9, 634, 10, 723, 11, 664, 12, 491, 3, 4, 5, 14]
20	α^2	α^4	α^7	α^{14}	4	17	[0, 1, 4, 17, 5, 68, 6, 164, 7, 294, 8, 471, 9, 678, 10, 720, 11, 636, 12, 515, 2, 4, 8, 9]
3	α^1	α^3	α^{10}	α^{12}	4	17	[0, 1, 4, 17, 5, 70, 6, 151, 7, 308, 8, 495, 9, 634, 10, 723, 11, 664, 12, 491, 1, 2, 10, 13]
13	α^1	α^9	α^{11}	α^{14}	4	17	[0, 1, 4, 17, 5, 70, 6, 151, 7, 308, 8, 495, 9, 634, 10, 723, 11, 664, 12, 491, 1, 9, 12, 13]
5	α^1	α^3	α^5	α^8	4	17	[0, 1, 4, 17, 5, 68, 6, 164, 7, 294, 8, 471, 9, 678, 10, 720, 11, 636, 12, 515, 1, 3, 5, 9]
45	α^7	α^8	α^{10}	α^{12}	4	17	[0, 1, 4, 17, 5, 68, 6, 164, 7, 294, 8, 471, 9, 678, 10, 720, 11, 636, 12, 515, 7, 8, 10, 13]
49	α^8	α^{10}	α^{13}	α^{14}	4	17	[0, 1, 4, 17, 5, 70, 6, 151, 7, 308, 8, 495, 9, 634, 10, 723, 11, 664, 12, 491, 8, 11, 12, 13]
23	α^2	α^5	α^{12}	α^{13}	4	17	[0, 1, 4, 17, 5, 68, 6, 164, 7, 294, 8, 471, 9, 678, 10, 720, 11, 636, 12, 515, 2, 5, 12, 14]
21	α^2	α^5	α^6	α^7	4	17	[0, 1, 4, 17, 5, 70, 6, 151, 7, 308, 8, 495, 9, 634, 10, 723, 11, 664, 12, 491, 2, 5, 6, 8]
12	α^1	α^8	α^{13}	α^{14}	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 1, 9, 10, 11]
0	α^1	α^2	α^3	α^{10}	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 1, 2, 3, 11]
41	α^5	α^6	α^7	α^8	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 5, 6, 7, 9]
47	α^7	α^{12}	α^{13}	α^{14}	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 8, 9, 10, 11]
2	α^1	α^2	α^9	α^{14}	4	18	[0, 1, 4, 18, 5, 72, 6, 145, 7, 300, 8, 510, 9, 644, 10, 703, 11, 664, 12, 506, 1, 2, 10, 11]
22	α^2	α^5	α^6	α^{12}	4	19	[0, 1, 4, 19, 5, 66, 6, 148, 7, 308, 8, 492, 9, 648, 10, 728, 11, 648, 12, 492, 2, 5, 6, 13]
32	α^3	α^5	α^8	α^9	4	19	[0, 1, 4, 19, 5, 66, 6, 148, 7, 308, 8, 492, 9, 648, 10, 728, 11, 648, 12, 492, 3, 5, 8, 10]
42	α^6	α^7	α^{11}	α^{14}	4	19	[0, 1, 4, 19, 5, 71, 6, 141, 7, 304, 8, 515, 9, 639, 10, 703, 11, 664, 12, 501, 6, 7, 12, 13]
39	α^4	α^7	α^8	α^{14}	4	19	[0, 1, 4, 19, 5, 71, 6, 141, 7, 304, 8, 515, 9, 639, 10, 703, 11, 664, 12, 501, 4, 7, 9, 10]
28	α^3	α^4	α^{10}	α^{11}	4	19	[0, 1, 4, 19, 5, 71, 6, 141, 7, 304, 8, 515, 9, 639, 10, 703, 11, 664, 12, 501, 3, 4, 10, 12]
43	α^6	α^9	α^{11}	α^{14}	4	19	[0, 1, 4, 19, 5, 66, 6, 148, 7, 308, 8, 492, 9, 648, 10, 728, 11, 648, 12, 492, 6, 9, 12, 13]
10	α^1	α^7	α^{10}	α^{12}	4	19	[0, 1, 4, 19, 5, 66, 6, 148, 7, 308, 8, 492, 9, 648, 10, 728, 11, 648, 12, 492, 1, 7, 10, 13]
9	α^1	α^7	α^8	α^{12}	4	19	[0, 1, 4, 19, 5, 71, 6, 141, 7, 304, 8, 515, 9, 639, 10, 703, 11, 664, 12, 501, 1, 7, 8, 13]
8	α^1	α^5	α^8	α^9	4	19	[0, 1, 4, 19, 5, 71, 6, 141, 7, 304, 8, 515, 9, 639, 10, 703, 11, 664, 12, 501, 1, 5, 8, 10]
29	α^3	α^4	α^{10}	α^{13}	4	19	[0, 1, 4, 19, 5, 66, 6, 148, 7, 308, 8, 492, 9, 648, 10, 728, 11, 648, 12, 492, 3, 4, 10, 14]
19	α^2	α^4	α^5	α^7	4	20	[0, 1, 4, 20, 5, 64, 6, 150, 7, 326, 8, 472, 9, 618, 10, 764, 11, 668, 12, 472, 2, 4, 5, 8]
7	α^1	α^3	α^{11}	α^{13}	4	20	[0, 1, 4, 20, 5, 64, 6, 150, 7, 326, 8, 472, 9, 618, 10, 764, 11, 668, 12, 472, 1, 3, 11, 14]
26	α^2	α^{10}	α^{12}	α^{14}	4	20	[0, 1, 4, 20, 5, 64, 6, 150, 7, 326, 8, 472, 9, 618, 10, 764, 11, 668, 12, 472, 2, 10, 13, 14]
48	α^8	α^{10}	α^{12}	α^{13}	4	20	[0, 1, 4, 20, 5, 64, 6, 150, 7, 326, 8, 472, 9, 618, 10, 764, 11, 668, 12, 472, 8, 10, 12, 14]
17	α^2	α^3	α^5	α^{13}	4	20	[0, 1, 4, 20, 5, 64, 6, 150, 7, 326, 8, 472, 9, 618, 10, 764, 11, 668, 12, 472, 2, 3, 5, 14]
50	α^{10}	α^{12}	α^{13}	α^{14}	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 11, 12, 13, 14]
1	α^1	α^2	α^3	α^{13}	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 1, 2, 3, 14]
4	α^1	α^2	α^{12}	α^{14}	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 1, 2, 13, 14]
14	α^1	α^{11}	α^{13}	α^{14}	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 1, 12, 13, 14]
15	α^2	α^3	α^4	α^5	4	21	[0, 1, 4, 21, 5, 63, 6, 152, 7, 312, 8, 479, 9, 655, 10, 728, 11, 648, 12, 503, 2, 3, 4, 6]
40	α^4	α^7	α^{10}	α^{13}	4	23	[0, 1, 4, 23, 5, 61, 6, 145, 7, 316, 8, 491, 9, 657, 10, 711, 11, 640, 12, 521, 4, 7, 10, 14]
46	α^7	α^{10}	α^{12}	α^{13}	4	23	[0, 1, 4, 23, 5, 56, 6, 154, 7, 320, 8, 479, 9, 664, 10, 700, 11, 640, 12, 537, 7, 10, 12, 14]
6	α^1	α^3	α^{10}	α^{13}	4	23	[0, 1, 4, 23, 5, 56, 6, 154, 7, 320, 8, 479, 9, 664, 10, 700, 11, 640, 12, 537, 1, 3, 10, 14]
30	α^3	α^5	α^6	α^8	4	23	[0, 1, 4, 23, 5, 56, 6, 154, 7, 320, 8, 479, 9, 664, 10, 700, 11, 640, 12, 537, 3, 5, 6, 9]
25	α^2	α^9	α^{12}	α^{14}	4	23	[0, 1, 4, 23, 5, 56, 6, 154, 7, 320, 8, 479, 9, 664, 10, 700, 11, 640, 12, 537, 2, 9, 13, 14]
36	α^3	α^6	α^8	α^{11}	4	23	[0, 1, 4, 23, 5, 61, 6, 145, 7, 316, 8, 491, 9, 657, 10, 711, 11, 640, 12, 521, 3, 6, 9, 12]
35	α^3	α^6	α^8	α^{12}	4	23	[0, 1, 4, 23, 5, 61, 6, 145, 7, 316, 8, 491, 9, 657, 10, 711, 11, 640, 12, 521, 3, 6, 8, 13]
33	α^3	α^5	α^9	α^{12}	4	23	[0, 1, 4, 23, 5, 61, 6, 145, 7, 316, 8, 491, 9, 657, 10, 711, 11, 640, 12, 521, 3, 5, 9, 13]
24	α^2	α^6	α^9	α^{12}	4	23	[0, 1, 4, 23, 5, 61, 6, 145, 7, 316, 8, 491, 9, 657, 10, 711, 11, 640, 12, 521, 2, 6, 9, 13]
16	α^2	α^3	α^5	α^{12}	4	23	[0, 1, 4, 23, 5, 56, 6, 154, 7, 320, 8, 479, 9, 664, 10, 700, 11, 640, 12, 537, 2, 3, 5, 13]
18	α^2	α^3	α^9	α^{12}	4	24	[0, 1, 4, 24, 5, 60, 6, 134, 7, 336, 8, 498, 9, 620, 10, 742, 11, 640, 12, 480, 2, 3, 9, 13]
11	α^1	α^7	α^{10}	α^{13}	4	24	[0, 1, 4, 24, 5, 60, 6, 134, 7, 336, 8, 498, 9, 620, 10, 742, 11, 640, 12, 480, 1, 7, 10, 14]
44	α^6	α^9	α^{12}	α^{14}	4	24	[0, 1, 4, 24, 5, 60, 6, 134, 7, 336, 8, 498, 9, 620, 10, 742, 11, 640, 12, 480, 6, 9, 13, 14]
34	α^3	α^6	α^8	α^9	4	24	[0, 1, 4, 24, 5, 60, 6, 134, 7, 336, 8, 498, 9, 620, 10, 742, 11, 640, 12, 480, 3, 6, 8, 10]
31	α^3	α^5	α^6	α^{12}	4	24	[0, 1, 4, 24, 5, 60, 6, 134, 7, 336, 8, 498, 9, 620, 10, 742, 11, 640, 12, 480, 3, 5, 6, 13]
37	α^3	α^6	α^9	α^{12}	4	25	[0, 1, 4, 25, 5, 64, 6, 120, 7, 320, 8, 550, 9, 640, 10, 656, 11, 640, 12, 550, 3, 6, 9, 13]

2.2 Optimal codes for (5,2)-SSS-based masking

As shown in our paper, the codes satifying two conditions are optimal:

- Maximizing $d_{\mathcal{D}}^{\perp}$, here $\max\{d_{\mathcal{D}}^{\perp}\}=4$
- Minimizing $B_{d_{\mathcal{D}}^{\perp}}$, here $\min\{B_{d_{\mathcal{D}}^{\perp}}\}=17$

Note that we use two complementary metrics **SNR** (signal-to-noise ratio) and **MI** (mutual information) to assess the side-channel resistance of SSS-based masking with different codes.

As a result of Tab. II, we conclude that the optimal codes for (5,2)-SSS based masking are generated by $\mathbf{H}=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2\end{pmatrix}$ where there are nine optimal codes with different $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)$. Note that permutation on five public points does not change the codes due to equivalence.

The generator matrices of the *all ten* codes are:

- $(\alpha_1,\alpha_3,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^3,\alpha^{10},\alpha^{11},\alpha^{13})$

$$\mathbf{H}_1=\begin{pmatrix}1 & \alpha^3 & \alpha^{10} & \alpha^{11} & \alpha^{13}\\ 1 & \alpha^6 & \alpha^5 & \alpha^7 & \alpha^{11}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&0&1&0&0&0&1&0&1&1&0&1\\0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&1&1&0&1&0\\0&0&1&0&0&0&0&0&1&1&1&0&1&1&0&0&0&1&0&1\\0&0&0&1&0&0&0&0&1&1&1&0&1&1&0&1&1&1&1&0\\0&0&0&0&1&0&0&0&1&0&1&1&0&0&1&1&0&0&1&0\\0&0&0&0&0&1&0&0&1&0&0&1&1&1&0&1&0&0&0&1\\0&0&0&0&0&0&1&0&1&0&0&0&1&0&1&0&1&1&0&0\\0&0&0&0&0&0&0&1&0&1&0&0&0&1&0&1&0&1&1&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^3,\alpha^4,\alpha^5,\alpha^{13})$

$$\mathbf{H}_2=\begin{pmatrix}1 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^{13}\\ 1 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{11}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&1&1&1&0&0&1&0&1&1&0&1\\0&1&0&0&0&0&0&0&1&0&1&1&0&0&0&1&1&0&1&0\\0&0&1&0&0&0&0&0&1&0&0&1&1&1&0&0&0&1&0&1\\0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&0&1&1&1&0\\0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&1&0&1&0\\0&0&0&0&0&1&0&0&1&1&0&0&1&0&0&1&0&0&0&1\\0&0&0&0&0&0&1&0&0&1&1&0&1&0&0&0&1&1&0&0\\0&0&0&0&0&0&0&1&0&0&1&1&0&1&0&0&0&1&1&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^2,\alpha^4,\alpha^7,\alpha^{14})$

$$\mathbf{H}_3=\begin{pmatrix}1 & \alpha^2 & \alpha^4 & \alpha^7 & \alpha^{14}\\ 1 & \alpha^4 & \alpha^8 & \alpha^{14} & \alpha^{13}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&1&1&0&0\\0&1&0&0&0&0&0&0&1&1&0&1&1&1&1&1&0&1&1&0\\0&0&1&0&0&0&0&0&1&0&1&0&1&0&1&1&0&0&1&1\\0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&1&1&1&0&1\\0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&1&1&1&0&1\\0&0&0&0&0&1&0&0&0&1&1&1&1&1&1&0&1&1&0&1&0\\0&0&0&0&0&0&1&0&1&1&1&1&1&0&1&0&0&1&0&1\\0&0&0&0&0&0&0&1&1&0&1&1&0&1&0&1&1&1&1&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^1,\alpha^2,\alpha^{10},\alpha^{12})$

$$\mathbf{H}_4=\begin{pmatrix}1 & \alpha^1 & \alpha^2 & \alpha^{10} & \alpha^{12}\\ 1 & \alpha^2 & \alpha^4 & \alpha^5 & \alpha^9\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&1&1\\0&1&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1&1&0&1\\0&0&1&0&0&0&0&0&1&1&0&0&1&0&0&1&0&1&0\\0&0&0&1&0&0&0&0&0&1&1&0&0&1&0&0&1&0&1\\0&0&0&0&1&0&0&0&0&1&1&0&1&1&1&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&1&1&0&1&1&1&1&1&0&0\\0&0&0&0&0&0&1&0&1&1&0&1&1&1&1&1&0&1&1&0\\0&0&0&0&0&0&0&1&1&0&1&0&1&0&1&1&0&0&1&1\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^1,\alpha^9,\alpha^{11},\alpha^{14})$

$$\mathbf{H}_5=\begin{pmatrix}1 & \alpha^1 & \alpha^9 & \alpha^{11} & \alpha^{14}\\ 1 & \alpha^2 & \alpha^3 & \alpha^7 & \alpha^{13}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&0&1&0&1&0&1&1&0&0&1&0\\0&1&0&0&0&0&0&0&0&1&0&1&1&0&0&1&0&0&0&1\\0&0&1&0&0&0&0&1&1&1&0&1&0&0&0&1&1&0&0\\0&0&0&1&0&0&0&0&1&1&1&0&1&0&0&0&1&1&0\\0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&1&1&1&1&1\\0&0&0&0&0&1&0&0&1&1&1&1&1&1&1&0&0&1&0&1&1\\0&0&0&0&0&0&1&0&1&0&1&1&0&1&1&0&1&0&0&1\\0&0&0&0&0&0&0&1&1&0&0&1&0&0&1&1&1&0&0&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^1,\alpha^3,\alpha^5,\alpha^8)$

$$\mathbf{H}_6=\begin{pmatrix}1 & \alpha^1 & \alpha^3 & \alpha^5 & \alpha^8\\ 1 & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^1\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&1&1&0&0&1\\0&1&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&0&0&0\\0&0&1&0&0&0&0&1&1&1&0&0&1&1&0&0&1&0&0\\0&0&0&1&0&0&0&0&1&1&1&0&0&1&1&0&0&1&0\\0&0&0&0&1&0&0&0&1&1&1&1&1&1&1&0&0&1&1&0\\0&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0&0&1&1\\0&0&0&0&0&0&1&0&1&0&0&1&1&1&1&1&1&1&0&1\\0&0&0&0&0&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^7,\alpha^8,\alpha^{10},\alpha^{12})$

$$\mathbf{H}_7=\begin{pmatrix}1 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{12}\\ 1 & \alpha^{14} & \alpha^1 & \alpha^5 & \alpha^9\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&1&1&0\\0&1&0&0&0&0&0&0&0&1&1&1&1&0&1&0&0&0&1&1\\0&0&1&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&0&1\\0&0&0&1&0&0&0&0&1&0&1&1&1&1&1&0&1&0&1&0\\0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&1&1&0&1\\0&0&0&0&0&1&0&0&1&1&1&0&1&0&0&0&1&0&1&0\\0&0&0&0&0&0&1&0&0&1&1&1&0&1&0&0&0&1&0&1\\0&0&0&0&0&0&0&1&1&1&1&1&0&0&1&0&1&1&1&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^8,\alpha^{10},\alpha^{13},\alpha^{14})$

$$\mathbf{H}_8=\begin{pmatrix}1 & \alpha^8 & \alpha^{10} & \alpha^{13} & \alpha^{14}\\ 1 & \alpha^1 & \alpha^5 & \alpha^{11} & \alpha^{13}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&1&0&0&0&1\\0&1&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&0&0\\0&0&1&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&0\\0&0&0&1&0&0&0&0&1&1&1&1&0&0&1&0&0&0&1&1\\0&0&0&0&1&0&0&0&0&1&1&0&0&1&0&1&1&1&0&1\\0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&1&0&1&0\\0&0&0&0&0&0&1&0&1&1&0&1&0&1&1&1&0&1&0&1\\0&0&0&0&0&0&0&1&1&0&1&0&1&1&1&1&1&1&1&0\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^2,\alpha^5,\alpha^{12},\alpha^{13})$

$$\mathbf{H}_9=\begin{pmatrix}1 & \alpha^2 & \alpha^5 & \alpha^{12} & \alpha^{13}\\ 1 & \alpha^4 & \alpha^{10} & \alpha^9 & \alpha^{11}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&1&1&0&0\\0&1&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&1&1&0\\0&0&1&0&0&0&0&0&1&0&0&0&1&0&1&1&0&0&1&1\\0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&1&1&1&0&1\\0&0&0&0&1&0&0&0&0&1&1&0&1&0&1&1&0&1&0&1\\0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&1&1&1&1&0\\0&0&0&0&0&0&1&0&1&1&0&1&1&0&0&0&0&1&1&1\\0&0&0&0&0&0&0&1&1&0&1&0&0&1&0&0&1&1&1&1\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$

- $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(1,\alpha^2,\alpha^5,\alpha^6,\alpha^7)$

$$\mathbf{H}_{10}=\begin{pmatrix}1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha^7\\ 1 & \alpha^4 & \alpha^{10} & \alpha^{12} & \alpha^{14}\end{pmatrix}\in\mathbb{F}_{2^4}^{2\times5}=\begin{pmatrix}1&0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&0&1&1&1\\0&1&0&0&0&0&0&0&1&0&0&1&0&0&1&0&1&1&1&1\\0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1\\0&0&0&1&0&0&0&0&0&1&0&0&1&1&0&0&1&0&0&1\\0&0&0&0&1&0&0&0&1&1&0&0&1&0&1&0&0&1&1\\0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&1&1&0&1\\0&0&0&0&0&0&1&0&1&1&1&0&1&0&1&1&1&1&0&1&0\\0&0&0&0&0&0&0&1&1&0&1&0&1&1&1&1&0&1&0&1\end{pmatrix}\in\mathbb{F}_2^{8\times20}$$