Test vectors for Rainbow (v1,o1,o2) = (2,2,2) over the field F_{31}

Private linear transformation: $S \in {F_{31}}^{n \times n}$

[2, 6, 26, 7, 1, 10,
18, 25, 30, 23, 17, 15,
5, 3, 13, 26, 7, 18,
6, 16, 19, 10, 29, 30,
22, 26, 0, 16, 28, 21,
22, 24, 6, 20, 2, 20]

Private quadratic maps: $F_1, \cdots, F_m \in {F_{31}}^{n \times n}$

F[1];
[29, 10, 16, 23, 0, 0,
0, 13, 16, 19, 0, 0,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0]

F[2];
[9, 21, 5, 4, 0, 0,
0, 10, 18, 17, 0, 0,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0]

F[3];
[14, 8, 28, 30, 7, 20,
0, 26, 26, 24, 28, 27,
0, 0, 0, 25, 4, 29,
0, 0, 0, 5, 9, 30,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0]

F[4];
[26, 10, 0, 16, 7, 12,
0, 18, 7, 8, 17, 4,
0, 0, 13, 29, 12, 23,
0, 0, 0, 7, 1, 8,
0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0]

Respective public keys $P_1, \cdots, P_m \in F_{31}{}^{n \times n}$

P[1]
[6, 9, 22, 27, 29, 1,
[6, 23, 6, 4, 26, 4,
[24, 14, 29, 29, 10, 17,
4, 23, 10, 10, 12, 8,
3, 19, 21, 24, 28, 18,
20, 15, 27, 15, 15, 23]

P[2]
[22, 16, 16, 29, 3, 17,
4, 26, 6, 24, 6, 10,
10, 4, 0, 22, 25, 17,
12, 11, 0, 14, 30, 8,
30, 25, 22, 6, 19, 9,
7, 19, 5, 26, 9, 28]

P[3]
[1, 9, 16, 24, 2, 12,
26, 29, 5, 17, 29, 1,
23, 18, 9, 5, 8, 11,
21, 22, 15, 12, 24, 29,
22, 23, 13, 22, 20, 28,
4, 10, 5, 11, 6, 12]

P[4]
[22, 16, 17, 5, 14, 6,
0, 18, 8, 12, 8, 7,
0, 8, 15, 6, 30, 4,
24, 8, 28, 23, 20, 21,
6, 9, 30, 20, 18, 26,
16, 19, 27, 11, 2, 18]

Hash of some message to be signed: $h(m) \in F_{31}{}^{m}$

h := Vector(K, [4, 16, 26, 30]);

One (among many) possible valid signature under private key given by S **and** F **'s above and hash** h**:**

s := Vector(K,[14, 9, 27, 3, 12, 16]);