TABLE I
1^{st} DIFFERENTIAL CHARACTERISTIC OF 21-ROUND ($p = 2^{-40}$)

Round	ΔX_i^L	ΔX_i^R	Probability
1	0000 0000	0000 0001	1
2	0000 0001	0000 0000	2^{-3}
3	1000 0000	0000 0001	2^{-2}
4	0000 0009	1000 0000	2^{-3}
5	0000 0000	0000 0009	1
6	0000 0009	0000 0000	2^{-3}
7	1000 0000	0000 0009	2^{-2}
8	0000 0001	1000 0000	2^{-3}
9	0000 0000	0000 0001	1
10	0000 0001	0000 0000	2^{-3}
11	1000 0000	0000 0001	2^{-2}
12	0000 0009	1000 0000	2^{-3}
13	0000 0000	0000 0009	1
14	0000 0009	0000 0000	2^{-3}
15	1000 0000	0000 0009	2^{-2}
16	0000 0001	1000 0000	2^{-3}
17	0000 0000	0000 0001	1
18	0000 0001	0000 0000	2^{-3}
19	1000 0000	0000 0001	2^{-2}
20	0000 0009	1000 0000	2^{-3}
21	0000 0000	0000 0009	1
Output	0000 0009	0000 0000	

TABLE II
2^{nd} DIFFERENTIAL CHARACTERISTIC OF 21-ROUND ($p = 2^{-40}$)

Round	ΔX_i^L	ΔX_i^R	Probability
1	0000 0000	0500 0000	1
2	0500 0000	0000 0000	2^{-3}
3	0000 2000	0500 0000	2^{-2}
4	0700 0000	0000 2000	2^{-3}
5	0000 0000	0700 0000	1
6	0700 0000	0000 0000	2^{-3}
7	0000 2000	0700 0000	2^{-2}
8	0500 0000	0000 2000	2^{-3}
9	0000 0000	0500 0000	1
10	0500 0000	0000 0000	2^{-3}
11	0000 2000	0500 0000	2^{-2}
12	0700 0000	0000 2000	2^{-3}
13	0000 0000	0700 0000	1
14	0700 0000	0000 0000	2^{-3}
15	0000 2000	0700 0000	2^{-2}
16	0500 0000	0000 2000	2^{-3}
17	0000 0000	0500 0000	1
18	0500 0000	0000 0000	2^{-3}
19	0000 2000	0500 0000	2^{-2}
20	0700 0000	0000 2000	2^{-3}
21	0000 0000	0700 0000	1
Output	0700 0000	0000 0000	

TABLE III
1^{st} DIFFERENTIAL CHARACTERISTIC OF 20-ROUND ($p = 2^{-40}$)

Round	ΔX_i^L	ΔX_i^R	Probability
1	0000 0001	0000 0000	2^{-3}
2	1000 0000	0000 0001	2^{-2}
3	0000 0009	1000 0000	2^{-3}
4	0000 0000	0000 0009	1
5	0000 0009	0000 0000	2^{-3}
6	1000 0000	0000 0009	2^{-2}
7	0000 0001	1000 0000	2^{-3}
8	0000 0000	0000 0001	1
9	0000 0001	0000 0000	2^{-3}
10	1000 0000	0000 0001	2^{-2}
11	0000 0009	1000 0000	2^{-3}
12	0000 0000	0000 0009	1
13	0000 0009	0000 0000	2^{-3}
14	1000 0000	0000 0009	2^{-2}
15	0000 0001	1000 0000	2^{-3}
16	0000 0000	0000 0001	1
17	0000 0001	0000 0000	2^{-3}
18	1000 0000	0000 0001	2^{-2}
19	0000 0009	1000 0000	2^{-3}
20	0000 0000	0000 0009	1
Output	0000 0009	0000 0000	

TABLE IV
2^{nd} DIFFERENTIAL CHARACTERISTIC OF 20-ROUND ($p = 2^{-40}$)

Round	ΔX_i^L	ΔX_i^R	Probability
1	0500 0000	0000 0000	2^{-3}
2	0000 2000	0500 0000	2^{-2}
3	0700 0000	0000 2000	2^{-3}
4	0000 0000	0700 0000	1
5	0700 0000	0000 0000	2^{-3}
6	0000 2000	0700 0000	2^{-2}
7	0500 0000	0000 2000	2^{-3}
8	0000 0000	0500 0000	1
9	0500 0000	0000 0000	2^{-3}
10	0000 2000	0500 0000	2^{-2}
11	0700 0000	0000 2000	2^{-3}
12	0000 0000	0700 0000	1
13	0700 0000	0000 0000	2^{-3}
14	0000 2000	0700 0000	2^{-2}
15	0500 0000	0000 2000	2^{-3}
16	0000 0000	0500 0000	1
17	0500 0000	0000 0000	2^{-3}
18	0000 2000	0500 0000	2^{-2}
19	0700 0000	0000 2000	2^{-3}
20	0000 0000	0700 0000	1
Output	0700 0000	0000 0000	

TABLE V
1^{st} DIFFERENTIAL CHARACTERISTIC OF 19-ROUND ($p = 2^{-37}$)

Round	ΔX_i^L	ΔX_i^R	Probability
1	0000 0000	0000 0001	1
2	0000 0001	0000 0000	2^{-3}
3	1000 0000	0000 0001	2^{-2}
4	0000 0009	1000 0000	2^{-3}
5	0000 0000	0000 0009	1
6	0000 0009	0000 0000	2^{-3}
7	1000 0000	0000 0009	2^{-2}
8	0000 0001	1000 0000	2^{-3}
9	0000 0000	0000 0001	1
10	0000 0001	0000 0000	2^{-3}
11	1000 0000	0000 0001	2^{-2}
12	0000 0009	1000 0000	2^{-3}
13	0000 0000	0000 0009	1
14	0000 0009	0000 0000	2^{-3}
15	1000 0000	0000 0009	2^{-2}
16	0000 0001	1000 0000	2^{-3}
17	0000 0000	0000 0001	1
18	0000 0001	0000 0000	2^{-3}
19	1000 0000	0000 0001	2^{-2}
Output	0000 0009	1000 0000	2^{-3}

TABLE VI
2^{nd} DIFFERENTIAL CHARACTERISTIC OF 19-ROUND ($p = 2^{-37}$)

Round	ΔX_i^L	ΔX_i^R	Probability
1	0000 0000	0500 0000	1
2	0500 0000	0000 0000	2^{-3}
3	0000 2000	0500 0000	2^{-2}
4	0700 0000	0000 2000	2^{-3}
5	0000 0000	0700 0000	1
6	0700 0000	0000 0000	2^{-3}
7	0000 2000	0700 0000	2^{-2}
8	0500 0000	0000 2000	2^{-3}
9	0000 0000	0500 0000	1
10	0500 0000	0000 0000	2^{-3}
11	0000 2000	0500 0000	2^{-2}
12	0700 0000	0000 2000	2^{-3}
13	0000 0000	0700 0000	1
14	0700 0000	0000 0000	2^{-3}
15	0000 2000	0700 0000	2^{-2}
16	0500 0000	0000 2000	2^{-3}
17	0000 0000	0500 0000	1
18	0500 0000	0000 0000	2^{-3}
19	0000 2000	0500 0000	2^{-2}
Output	0700 0000	0000 2000	2^{-3}