

TABLE 4 LEAKAGE OF FOUR-INPUT, FOUR-OUTPUT CRYPTOGRAPHIC CORE FOR ALL POSSIBLE INPUTS

Key 0 (0 0 0 0)			Key 1 (0 0 0 1)			Key 2 (0 0 1 0)			Key 3 (0 0 1 1)		
OUT	IN	nA	OUT	IN	nA	OUT	IN	nA	OUT	IN	nA
1 1 0 1	1 0 0 1	666	1 1 1 1	0 1 0 0	653.7	1 1 0 1	1 0 0 1	646.8	1 1 1 1	0 1 0 0	634.5
1 1 1 1	0 1 0 0	672.8	1 0 0 0	1 0 0 0	659.7	1 1 1 1	0 1 0 0	653.7	1 0 0 0	1 0 0 0	640.5
1 1 0 0	1 1 1 1	673.9	1 1 0 1	1 0 0 1	662.4	1 1 1 0	0 0 0 1	656.3	1 1 0 1	1 0 0 1	643.3
1 1 1 0	0 0 0 1	675.5	0 0 0 1	1 1 0 0	662.8	1 0 0 0	1 0 0 0	659.7	0 0 0 1	1 1 0 0	643.7
0 0 0 0	1 0 1 1	676.5	0 0 1 1	0 0 0 0	663.9	0 0 0 1	1 1 0 0	662.8	0 0 1 1	0 0 0 0	644.8
1 0 0 0	1 0 0 0	678.8	0 1 1 0	1 0 1 0	668.1	0 0 1 1	0 0 0 0	663.9	1 1 1 0	0 0 0 1	652.8
0 0 0 1	1 1 0 0	682	1 1 0 0	1 1 1 1	670.4	0 0 1 0	1 1 0 1	664.6	0 0 1 0	1 1 0 1	661.1
0 1 1 1	0 0 1 1	682.1	1 0 1 1	1 1 1 0	671	1 1 0 0	1 1 1 1	670.4	0 1 1 0	1 0 1 0	664.6
0 0 1 1	0 0 0 0	683	1 0 1 0	0 0 1 0	671.8	0 1 0 0	0 1 0 1	671.6	1 1 0 0	1 1 1 1	666.8
0 0 1 0	1 1 0 1	683.8	1 1 1 0	0 0 0 1	671.9	0 0 0 0	1 0 1 1	672.9	1 0 1 1	1 1 1 0	667.5
0 1 1 0	1 0 1 0	687.3	0 0 0 0	1 0 1 1	672.9	0 1 1 1	0 0 1 1	678.5	0 1 0 0	0 1 0 1	668
1 0 1 1	1 1 1 0	690.2	0 1 0 1	0 1 1 0	675.3	0 1 1 0	1 0 1 0	683.7	1 0 1 0	0 0 1 0	668.2
0 1 0 0	0 1 0 1	690.7	0 1 1 1	0 0 1 1	678.5	1 0 1 1	1 1 1 0	686.6	0 0 0 0	1 0 1 1	669.3
1 0 1 0	0 0 1 0	690.9	0 0 1 0	1 1 0 1	680.2	1 0 1 0	0 0 1 0	687.3	0 1 0 1	0 1 1 0	671.8
1 0 0 1	0 1 1 1	693	0 1 0 0	0 1 0 1	687.2	1 0 0 1	0 1 1 1	689.4	0 1 1 1	0 0 1 1	674.9
0 1 0 1	0 1 1 0	694.5	1 0 0 1	0 1 1 1	689.4	0 1 0 1	0 1 1 0	690.9	1 0 0 1	0 1 1 1	685.8
Key 4 (0 1 0 0)			Key 5 (0 1 0 1)			Key 6 (0 1 1 0)			Key 7 (0 1 1 1)		
OUT	IN	nA	OUT	IN	nA	OUT	IN	nA	OUT	IN	nA
1 1 0 1	1 0 0 1	646.8	1 0 0 0	1 0 0 0	640.5	1 1 0 1	1 0 0 1	627.7	1 0 0 0	1 0 0 0	621.4
1 1 1 0	0 0 0 1	656.3	1 1 0 1	1 0 0 1	643.3	1 1 1 0	0 0 0 1	637.2	1 1 0 1	1 0 0 1	624.1
0 0 0 0	1 0 1 1	657.3	0 0 1 1	0 0 0 0	644.8	1 0 0 0	1 0 0 0	640.5	0 0 1 1	0 0 0 0	625.6
1 0 0 0	1 0 0 0	659.7	0 1 1 0	1 0 1 0	649	0 0 1 1	0 0 0 0	644.8	1 1 1 1	0 1 0 0	631
0 1 1 1	0 0 1 1	662.9	1 1 1 1	0 1 0 0	650.1	1 1 1 1	0 1 0 0	650.1	1 1 1 0	0 0 0 1	633.6
0 0 1 1	0 0 0 0	663.9	1 0 1 0	0 0 1 0	652.6	0 0 0 0	1 0 1 1	653.8	0 0 0 1	1 1 0 0	640.1
0 1 1 0	1 0 1 0	668.2	1 1 1 0	0 0 0 1	652.8	0 0 0 1	1 1 0 0	659.3	0 1 1 0	1 0 1 0	645.4
1 1 1 1	0 1 0 0	669.2	0 0 0 0	1 0 1 1	652.8	0 1 1 1	0 0 1 1	659.4	1 0 1 0	0 0 1 0	649.1
1 1 0 0	1 1 1 1	670.4	0 0 0 1	1 1 0 0	659.3	0 0 1 0	1 1 0 1	661.1	0 0 0 0	1 0 1 1	650.2
1 0 1 0	0 0 1 0	671.8	0 1 1 1	0 0 1 1	659.4	0 1 1 0	1 0 1 0	664.6	0 1 1 1	0 0 1 1	655.8
0 0 0 1	1 1 0 0	678.4	1 1 0 0	1 1 1 1	666.8	1 1 0 0	1 1 1 1	666.8	0 0 1 0	1 1 0 1	657.5
0 0 1 0	1 1 0 1	680.2	1 0 1 1	1 1 1 0	667.5	0 1 0 0	0 1 0 1	668	1 1 0 0	1 1 1 1	663.2
1 0 1 1	1 1 1 0	686.6	0 1 0 1	0 1 1 0	671.8	1 0 1 0	0 0 1 0	668.2	1 0 1 1	1 1 1 0	663.9
0 1 0 0	0 1 0 1	687.2	0 0 1 0	1 1 0 1	676.7	1 0 1 1	1 1 1 0	683	0 1 0 0	0 1 0 1	664.5
1 0 0 1	0 1 1 1	689.4	0 1 0 0	0 1 0 1	683.6	1 0 0 1	0 1 1 1	685.8	0 1 0 1	0 1 1 0	668.2
0 1 0 1	0 1 1 0	690.9	1 0 0 1	0 1 1 1	685.8	0 1 0 1	0 1 1 0	687.4	1 0 0 1	0 1 1 1	682.3

Key 8 (1 0 0 0)			Key 9 (1 0 0 1)			Key 10 (1 0 1 0)			Key 11 (1 0 1 1)		
OUT	IN	nA	OUT	IN	nA	OUT	IN	nA	OUT	IN	nA
1 1 1 1	0 1 0 0	653.7	1 1 1 1	0 1 0 0	634.5	1 1 1 1	0 1 0 0	634.5	1 1 1 1	0 1 0 0	615.4
1 1 1 0	0 0 0 1	656.3	0 0 1 1	0 0 0 0	644.8	1 1 1 0	0 0 0 1	637.2	0 0 1 1	0 0 0 0	625.6
1 1 0 1	1 0 0 1	662.4	1 0 1 0	0 0 1 0	652.6	1 1 0 1	1 0 0 1	643.3	1 1 1 0	0 0 0 1	633.6
0 1 1 1	0 0 1 1	662.9	1 1 1 0	0 0 0 1	652.8	0 0 1 1	0 0 0 0	644.8	1 0 0 0	1 0 0 0	637
0 0 1 1	0 0 0 0	663.9	1 0 0 0	1 0 0 0	656.1	0 1 0 0	0 1 0 1	652.5	1 1 0 1	1 0 0 1	639.7
1 1 0 0	1 1 1 1	670.4	0 1 0 1	0 1 1 0	656.2	1 0 0 0	1 0 0 0	656.1	0 0 0 1	1 1 0 0	640.1
0 1 0 0	0 1 0 1	671.6	1 1 0 1	1 0 0 1	658.8	0 0 0 1	1 1 0 0	659.3	0 1 0 0	0 1 0 1	648.9
1 0 1 0	0 0 1 0	671.8	0 0 0 1	1 1 0 0	659.3	0 1 1 1	0 0 1 1	659.4	1 0 1 0	0 0 1 0	649.1
0 0 0 0	1 0 1 1	672.9	0 1 1 1	0 0 1 1	659.4	0 0 1 0	1 1 0 1	661.1	0 1 0 1	0 1 1 0	652.6
1 0 0 1	0 1 1 1	673.8	0 1 1 0	1 0 1 0	664.6	1 1 0 0	1 1 1 1	666.8	0 1 1 1	0 0 1 1	655.8
1 0 0 0	1 0 0 0	675.2	1 1 0 0	1 1 1 1	666.8	1 0 1 0	0 0 1 0	668.2	0 0 1 0	1 1 0 1	657.5
0 1 0 1	0 1 1 0	675.3	1 0 1 1	1 1 1 0	667.5	0 0 0 0	1 0 1 1	669.3	0 1 1 0	1 0 1 0	661
0 0 0 1	1 1 0 0	678.4	0 1 0 0	0 1 0 1	668	1 0 0 1	0 1 1 1	670.3	1 1 0 0	1 1 1 1	663.2
0 0 1 0	1 1 0 1	680.2	0 0 0 0	1 0 1 1	669.3	0 1 0 1	0 1 1 0	671.8	1 0 1 1	1 1 1 0	663.9
0 1 1 0	1 0 1 0	683.7	1 0 0 1	0 1 1 1	670.3	0 1 1 0	1 0 1 0	680.2	0 0 0 0	1 0 1 1	665.8
1 0 1 1	1 1 1 0	686.6	0 0 1 0	1 1 0 1	676.7	1 0 1 1	1 1 1 0	683	1 0 0 1	0 1 1 1	666.7
Key 12 (1 1 0 0)			Key 13 (1 1 0 1)			Key 14 (1 1 1 0)			Key 15 (1 1 1 1)		
OUT	IN	nA	OUT	IN	nA	OUT	IN	nA	OUT	IN	nA
1 1 1 0	0 0 0 1	637.2	0 0 1 1	0 0 0 0	625.6	1 1 1 0	0 0 0 1	618.1	0 0 1 1	0 0 0 0	606.5
1 1 0 1	1 0 0 1	643.3	1 1 1 1	0 1 0 0	631	1 1 0 1	1 0 0 1	624.1	1 1 1 1	0 1 0 0	611.8
0 1 1 1	0 0 1 1	643.8	1 0 1 0	0 0 1 0	633.5	0 0 1 1	0 0 0 0	625.6	1 1 1 0	0 0 0 1	614.5
0 0 1 1	0 0 0 0	644.8	1 1 1 0	0 0 0 1	633.6	1 1 1 1	0 1 0 0	631	1 0 0 0	1 0 0 0	617.8
1 1 1 1	0 1 0 0	650.1	1 0 0 0	1 0 0 0	637	1 0 0 0	1 0 0 0	637	1 1 0 1	1 1 0 1	620.6
1 0 1 0	0 0 1 0	652.6	1 1 0 1	1 0 0 1	639.7	0 1 1 1	0 0 1 1	640.2	1 0 1 0	0 0 1 0	629.9
0 0 0 0	1 0 1 1	653.8	0 1 1 1	0 0 1 1	640.2	0 1 0 0	0 1 0 1	648.9	0 1 1 1	0 0 1 1	636.6
1 0 0 0	1 0 0 0	656.1	0 1 1 0	1 0 1 0	645.4	1 0 1 0	0 0 1 0	649.1	0 0 0 1	1 1 0 0	636.6
0 1 1 0	1 0 1 0	664.6	0 0 0 0	1 0 1 1	650.2	0 0 0 0	1 0 1 1	650.2	0 1 1 0	1 0 1 0	641.9
1 1 0 0	1 1 1 1	666.8	0 1 0 1	0 1 1 0	652.6	0 0 0 1	1 1 0 0	655.7	0 1 0 0	0 1 0 1	645.3
0 1 0 0	0 1 0 1	668	0 0 0 1	1 1 0 0	655.7	0 0 1 0	1 1 0 1	657.5	0 0 0 0	1 0 1 1	646.6
1 0 0 1	0 1 1 1	670.3	1 1 0 0	1 1 1 1	663.2	0 1 1 0	1 0 1 0	661	0 1 0 1	0 1 1 0	649.1
0 1 0 1	0 1 1 0	671.8	1 0 1 1	1 1 1 0	663.9	1 1 0 0	1 1 1 1	663.2	0 0 1 0	1 1 0 1	653.9
0 0 0 1	1 1 0 0	674.8	0 1 0 0	0 1 0 1	664.5	1 0 0 1	0 1 1 1	666.7	1 1 0 0	1 1 1 1	659.7
0 0 1 0	1 1 0 1	676.7	1 0 0 1	0 1 1 1	666.7	0 1 0 1	0 1 1 0	668.2	1 0 1 1	1 1 1 0	660.3
1 0 1 1	1 1 1 0	683	0 0 1 0	1 1 0 1	673.1	1 0 1 1	1 1 1 0	679.5	1 0 0 1	0 1 1 1	663.1