

### Appendix - The Difference Distribution Tables

### The Difference Distribution Table of S1

Input XOR	Output XOR															
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$
$0_0$	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$1_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$2_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$3_0$	14	4	2	2	0	0	0	0	0	0	0	0	0	0	0	0
$4_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$5_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$6_0$	0	4	2	4	0	0	0	0	0	0	0	0	0	0	0	0
$7_0$	2	4	10	4	0	0	0	0	0	0	0	0	0	0	0	0
$8_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$9_0$	10	2	4	0	2	4	6	0	0	0	0	0	0	0	0	0
$A_0$	0	8	6	2	2	8	6	0	0	0	0	0	0	0	0	0
$B_0$	2	4	0	10	2	2	4	0	0	0	0	0	0	0	0	0
$C_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$D_0$	6	6	4	8	4	8	2	6	0	0	0	0	0	0	0	0
$E_0$	0	4	8	8	10	2	4	0	0	0	0	0	0	0	0	0
$F_0$	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
$10_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$11_0$	6	8	2	4	6	8	6	4	0	0	0	0	0	0	0	0
$12_0$	0	8	4	2	6	6	0	4	6	6	4	2	6	6	0	4
$13_0$	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
$14_0$	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
$15_0$	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
$16_0$	0	8	10	8	0	0	2	2	6	10	2	0	2	6	6	2
$17_0$	4	4	6	10	6	0	2	4	4	6	0	2	6	0	6	6
$18_0$	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
$19_0$	2	6	2	4	0	8	4	6	10	4	0	2	8	4	4	0
$1A_0$	0	6	4	0	4	6	6	2	4	6	2	0	4	6	8	8
$1B_0$	4	2	4	10	6	6	4	6	2	2	4	2	4	2	4	2
$1C_0$	0	10	6	8	0	0	12	0	0	0	0	0	6	6	14	0
$1D_0$	4	0	8	2	6	0	0	0	0	0	0	0	6	6	14	0
$1E_0$	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
$1F_0$	2	4	10	6	2	2	0	0	6	8	0	0	0	4	6	4

### The Difference Distribution Table of S1 (cont.)

Input XOR	Output XOR																
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$	
$20_0$	0	0	0	0	10	0	12	8	2	0	6	4	4	4	2	6	12
$21_0$	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8	8
$22_0$	10	4	6	8	2	8	2	2	2	2	6	2	6	2	4	10	0
$23_0$	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10	0
$24_0$	12	0	0	2	2	2	0	14	14	2	0	2	0	2	6	2	4
$25_0$	6	4	4	12	4	4	4	10	2	2	2	2	2	4	2	2	2
$26_0$	0	0	4	10	10	2	4	0	4	6	4	4	4	4	2	0	0
$27_0$	10	2	2	0	2	2	0	4	8	0	4	8	4	0	4	0	2
$28_0$	12	2	2	0	2	6	12	0	0	2	6	0	4	0	0	6	2
$29_0$	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4	0
$2A_0$	4	2	4	6	0	2	8	2	14	2	6	2	6	2	6	2	2
$2B_0$	12	2	2	8	4	6	6	2	0	2	6	2	6	0	8	4	4
$2C_0$	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6	6
$2D_0$	6	2	8	2	8	4	4	2	4	6	0	8	2	2	6	6	6
$2E_0$	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4	2
$2F_0$	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2	2
$30_0$	0	4	6	0	12	6	2	2	6	0	0	2	2	4	10	8	0
$31_0$	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8	0
$32_0$	4	2	6	4	4	2	2	4	6	6	4	8	2	2	2	8	0
$33_0$	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4	4
$34_0$	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6	6
$35_0$	2	2	4	0	8	0	0	0	14	4	6	8	0	0	14	0	0
$36_0$	2	6	2	0	12	8	4	2	4	2	6	0	2	2	4	4	0
$37_0$	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4	4
$38_0$	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10	0
$39_0$	6	2	8	2	12	6	2	8	4	0	2	2	8	2	8	4	0
$3A_0$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0	0
$3B_0$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2	0
$3C_0$	0	10	6	0	12	8	4	2	4	0	2	6	0	2	6	0	0
$3D_0$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4	0
$3E_0$	4	8	2	2	4	4	14	4	2	0	0	0	0	8	4	0	6
$3F_0$	4	8	4	2	4	0	2	4	2	4	8	8	6	2	2	2	2

### The Difference Distribution Table of S2

Input XOR	Output XOR																
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$	
$0_0$	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$1_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$2_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$3_0$	4	8	4	8	4	6	4	2	4	2	2	4	6	2	0	4	
$4_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$5_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$6_0$	12	6	4	6	4	6	2	2	2	10	2	8	2	0	0	0	
$7_0$	4	0	4	8	2	4	6	2	4	2	4	2	4	2	4	2	
$8_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$9_0$	14	2	4	10	2	8	2	6	2	4	0	0	0	2	2	4	
$A_0$	8	6	4	2	4	10	2	10	2	0	0	0	0	2	4	0	
$B_0$	6	2	2	0	2	4	10	2	2	4	0	0	0	6	4	8	
$C_0$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
$D_0$	0	12	8	0	4	2	0	4	2	0	8	2	4	4	6	2	6
$E_0$	0	8	2	0	6	6	8	2	4	4	4	4	8	6	8	0	4
$F_0$	0	6	4	0	10	2	4	10	2	0	0	0	0	10	8	0	4
$10_0$	6	6	4	6	4	0	6	4	8	2	10	2	2	4	0	0	0
$11_0$	6	6	4	6	4	0	6	4	8	2	10	2	2	4	0	0	0
$12_0$	0	6	2	6	2	12	4	6	4	0	4	0	4	6	2	2	2
$13_0$	6	6	4	6	4	0	6	4	8	2	10	2	2	4	4	2	2
$14_0$	0	6	6	4	10	0	2	12	6	2	2	2	2	14	10	14	0
$15_0$	6	8	2	0	8	2	0	2	2	2	2	2	2	2	10	10	0
$16_0$	6	6	4	6	4	0	6	4	8	2	10	2	2	4	6	6	6
$17_0$	6	4	8	6	4	4	2	4	6	2	4	4	4	4	2	4	2
$18_0$	0	6	4	6	10	4	0	2	4	8	0	0	4	8	2	2	0
$19_0$	2	6	4	4	2	4	2	4	2	2	8	2	2	2	4	4	8
$1A_0$	0	6	8	4	2	4	2	2	8	2	2	2	6	2	4	4	6
$1B_0$	0	6	4	4	0	12	6	4	2	2	2	2	4	4	2	10	2
$1C_0$	4	6	4	6	2	4	6	12	0								

The Difference Distribution Table of S4 (cont.)

Input XOR	Output XOR															
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$
20 <sub>0</sub>	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21 <sub>0</sub>	0	4	8	0	8	4	0	8	4	0	4	0	4	0	8	0
22 <sub>0</sub>	8	0	4	8	0	4	8	0	4	8	0	4	8	0	4	8
23 <sub>0</sub>	4	0	2	8	0	2	0	2	0	2	0	2	0	2	0	2
24 <sub>0</sub>	0	6	6	4	6	4	0	6	6	4	0	6	4	6	6	0
25 <sub>0</sub>	0	8	4	4	0	0	4	8	8	0	8	4	8	4	0	4
26 <sub>0</sub>	0	6	2	0	6	4	8	0	6	2	0	6	4	2	0	6
27 <sub>0</sub>	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
28 <sub>0</sub>	16	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4
29 <sub>0</sub>	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
2A <sub>0</sub>	0	2	2	16	2	4	4	2	2	4	4	2	16	2	2	0
2B <sub>0</sub>	8	0	4	0	4	0	8	0	4	0	8	0	4	0	8	0
2C <sub>0</sub>	8	4	4	4	4	0	8	4	4	0	8	4	4	4	0	8
2D <sub>0</sub>	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
2E <sub>0</sub>	16	0	0	4	16	0	0	12	16	0	0	0	0	0	16	0
2F <sub>0</sub>	16	0	0	0	0	16	0	0	0	16	0	0	0	0	0	16
30 <sub>0</sub>	0	6	6	4	6	4	0	6	6	4	0	6	4	6	6	0
31 <sub>0</sub>	0	8	4	0	8	0	4	8	0	4	8	0	4	8	0	4
32 <sub>0</sub>	16	6	6	4	6	4	0	2	6	4	0	2	6	4	0	2
33 <sub>0</sub>	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
34 <sub>0</sub>	0	12	12	14	12	0	0	12	0	0	0	8	0	0	0	0
35 <sub>0</sub>	0	4	8	0	8	4	0	4	0	4	0	4	0	4	0	8
36 <sub>0</sub>	0	2	2	4	2	0	4	2	0	4	2	0	4	2	0	4
37 <sub>0</sub>	0	2	6	4	2	8	4	2	0	8	4	2	0	8	4	2
38 <sub>0</sub>	0	4	4	0	4	4	4	0	4	4	0	4	4	0	4	4
39 <sub>0</sub>	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
3A <sub>0</sub>	0	4	4	0	4	0	4	0	4	0	4	0	4	0	4	0
3B <sub>0</sub>	16	4	4	0	4	0	4	0	4	0	4	0	4	0	4	16
3C <sub>0</sub>	0	2	6	4	6	8	0	6	2	0	8	2	0	6	4	2
3D <sub>0</sub>	0	2	6	4	6	8	0	6	2	0	8	2	0	6	4	2
3E <sub>0</sub>	0	2	2	8	2	12	4	2	2	12	4	2	2	8	2	0
3F <sub>0</sub>	8	4	0	8	0	0	0	4	16	0	4	8	4	0	8	0

The Difference Distribution Table of S5

Input XOR	Output XOR															
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$
1 <sub>0</sub>	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2 <sub>0</sub>	0	0	0	4	0	10	8	6	0	4	2	2	12	10	2	4
3 <sub>0</sub>	0	0	0	4	0	10	6	4	0	6	4	4	0	8	10	6
4 <sub>0</sub>	0	0	0	8	0	4	2	4	0	8	2	4	0	8	10	6
5 <sub>0</sub>	0	0	0	8	0	4	2	4	0	8	2	4	0	8	10	6
6 <sub>0</sub>	12	0	0	4	0	10	6	4	0	6	4	4	0	16	0	0
7 <sub>0</sub>	0	8	4	6	4	6	2	2	0	4	0	6	0	0	6	10
8 <sub>0</sub>	2	0	4	8	4	2	6	6	2	8	8	0	8	10	4	0
9 <sub>0</sub>	0	0	0	4	0	10	6	4	0	6	4	4	0	16	0	0
A <sub>0</sub>	8	6	0	4	0	6	6	4	0	2	10	8	6	2	0	4
B <sub>0</sub>	4	2	2	4	8	10	8	4	2	6	2	2	6	2	2	0
C <sub>0</sub>	0	0	0	10	0	2	10	2	0	6	10	6	6	6	2	4
D <sub>0</sub>	10	4	2	2	0	6	16	0	0	2	10	2	2	4	0	4
E <sub>0</sub>	12	6	4	8	4	6	10	2	4	4	4	2	4	2	4	4
F <sub>0</sub>	4	4	0	8	0	2	0	2	8	2	4	2	8	4	4	12
10 <sub>0</sub>	0	0	0	0	0	4	12	0	2	8	10	4	6	12	2	0
11 <sub>0</sub>	6	6	10	10	4	0	2	16	2	4	0	6	2	4	2	0
12 <sub>0</sub>	0	2	4	2	10	4	0	10	8	6	0	6	0	6	6	0
13 <sub>0</sub>	0	0	6	2	8	0	0	4	4	6	2	8	2	8	10	4
14 <sub>0</sub>	0	12	2	6	2	0	4	4	8	4	4	4	6	6	2	0
15 <sub>0</sub>	4	8	0	2	8	0	2	2	4	2	2	4	2	4	8	6
16 <sub>0</sub>	0	6	10	2	14	0	2	2	4	4	0	6	0	4	6	4
17 <sub>0</sub>	0	10	8	0	6	4	0	2	2	4	0	2	2	4	0	6
18 <sub>0</sub>	0	10	8	0	6	4	0	2	2	4	0	2	2	4	0	6
19 <sub>0</sub>	0	4	6	2	4	4	2	6	4	4	2	2	4	12	2	10
1A <sub>0</sub>	0	16	2	12	2	0	6	2	0	6	4	0	4	0	4	8
1B <sub>0</sub>	0	18	12	0	0	2	2	6	8	4	0	6	0	0	8	6
1C <sub>0</sub>	0	2	6	6	6	6	6	4	8	2	0	6	4	4	2	0
1D <sub>0</sub>	0	2	6	6	6	6	6	4	8	2	0	6	4	4	2	0
1E <sub>0</sub>	0	2	6	6	6	6	6	4	8	2	0	6	4	4	2	0
1F <sub>0</sub>	0	6	8	4	8	8	0	6	2	2	0	6	0	10	10	4

The Difference Distribution Table of S5 (cont.)

Input XOR	Output XOR															
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$
20 <sub>0</sub>	0	0	0	0	0	8	2	6	0	4	4	4	6	6	8	8
21 <sub>0</sub>	0	0	0	6	6	2	6	4	6	10	14	4	0	0	0	4
22 <sub>0</sub>	14	4	0	10	0	2	12	2	2	10	2	0	0	0	2	2
23 <sub>0</sub>	2	0	0	4	2	2	10	4	0	8	8	2	6	8	0	8
24 <sub>0</sub>	6	2	8	4	4	4	6	2	2	6	6	2	6	2	2	2
25 <sub>0</sub>	6	0	0	4	2	8	2	6	6	4	2	4	2	6	6	6
26 <sub>0</sub>	12	0	0	4	0	4	4	0	8	4	0	12	8	0	4	0
27 <sub>0</sub>	0	2	4	2	0	2	2	4	4	4	8	4	8	4	0	4
28 <sub>0</sub>	2	8	4	6	2	4	6	0	6	6	4	0	2	2	2	10
29 <sub>0</sub>	6	4	6	8	8	4	6	2	0	2	2	10	0	2	4	0
2A <sub>0</sub>	4	6	2	6	0	12	2	0	4	12	2	10	4	4	12	4
2B <sub>0</sub>	8	6	2	6	4	8	6	0	4	4	0	2	6	0	6	2
2C <sub>0</sub>	6	0	2	4	0	6	6	4	2	10	6	10	6	2	0	0
2D <sub>0</sub>	10	4	0	2	2	6	10	2	2	2	4	6	2	2	2	10
2E <sub>0</sub>	0	4	0	10	2	0	0	4	0	4	0	4	0	4	6	12
2F <sub>0</sub>	0	6	6	4	10	2	0	0	4	0	0	4	6	12	6	6
30 <sub>0</sub>	4	6	0	2	6	4	6	0	6	0	4	6	4	10	6	0
31 <sub>0</sub>	0	6	6	4	10	2	0	0	4	0	0	4	0	4	6	12
32 <sub>0</sub>	4	6	0	2	6	4	6	0	6	0	4	6	4	10	6	0
33 <sub>0</sub>	8	10	0	14	8	0	8	2	2	4	0	4	0	4	4	0
34 <sub>0</sub>	0	4	4	2	14	4	0	8	6	8	2	2	0	4	6	0
35 <sub>0</sub>	0	4	16	0	8	4	0	4	4	0	8	0	4	4	4	4
36 <sub>0</sub>	4	4	4	2	0	2	12	2	4	8	4	2	2	6	2	4
37 <sub>0</sub>	4	2	2	2	4	2	0	8	2	2	2	12	6	2	8	6
38 <sub>0</sub>	0	4	8	4	12	0	0	8	10	2	0	0	0	4	2	10
39 <sub>0</sub>	0	8	12	0	4	6	0	0	6	2	10	8	0	0	4	6
3A <sub>0</sub>	0	14	4	0	4	6	0	0	6	2	10	8	0	0	4	6
3B <sub>0</sub>	0	2	2	4	4	8	6	8	2	2	2	6	14	2	0	0
3C <sub>0</sub>	0	0	10	2	4	8	6	2	2	10	4	10	8	8	0	0
3D <sub>0</sub>	0	6	12	2	4	8	0	8	8	2	2	0	2	2	4	4
3E <sub>0</sub>	4	4	10	0	2	4	8	8	2	2	0	2	6	8	4	0
3F <sub>0</sub>	8	6	6	0	4	2	2	4	2	8	6	2	4	2	4	0

The Difference Distribution Table of S6

**The Difference Distribution Table of S8 (cont.)**

Input NOR	Output NOR															
	$0_0$	$1_0$	$2_0$	$3_0$	$4_0$	$5_0$	$6_0$	$7_0$	$8_0$	$9_0$	$A_0$	$B_0$	$C_0$	$D_0$	$E_0$	$F_0$
20 <sub>r</sub>	0	0	0	10	0	4	0	0	0	14	6	4	2	0	4	14
21 <sub>r</sub>	0	0	2	10	2	8	10	0	0	6	6	0	10	2	2	6
22 <sub>r</sub>	8	0	6	0	6	4	10	2	0	6	8	0	4	4	2	4
23 <sub>r</sub>	4	8	0	6	0	4	8	6	2	2	10	4	8	0	0	2
24 <sub>r</sub>	4	0	4	8	4	6	2	4	8	6	2	0	0	4	4	8
25 <sub>r</sub>	0	4	6	8	2	8	8	0	4	2	4	4	2	2	6	4
26 <sub>r</sub>	2	6	0	6	4	4	6	6	0	4	4	10	4	2	2	2
27 <sub>r</sub>	6	6	0	0	2	2	6	2	4	4	6	10	2	6	2	6
28 <sub>r</sub>	10	2	6	2	4	12	12	0	2	2	4	0	0	0	2	6
29 <sub>r</sub>	4	0	0	14	2	10	4	2	8	6	4	0	4	2	2	2
2A <sub>r</sub>	8	8	0	2	0	2	4	0	2	6	8	14	2	8	0	0
2B <sub>r</sub>	2	2	0	0	4	2	10	4	6	2	4	0	6	4	8	10
2C <sub>r</sub>	2	6	6	2	4	6	2	0	2	6	4	0	6	4	10	4
2D <sub>r</sub>	8	0	4	4	6	2	0	0	6	8	2	4	6	4	4	6
2E <sub>r</sub>	6	2	2	4	2	2	6	12	4	0	4	2	8	8	0	2
2F <sub>r</sub>	8	12	4	6	6	4	2	2	2	2	4	2	2	4	0	4
30 <sub>r</sub>	0	4	6	2	10	2	2	2	4	8	0	0	8	4	6	6
31 <sub>r</sub>	4	6	8	0	4	6	0	4	6	10	2	2	4	4	0	0
32 <sub>r</sub>	6	6	6	2	4	6	0	2	0	6	8	2	2	6	6	2
33 <sub>r</sub>	6	6	4	2	4	0	0	10	2	2	0	6	8	4	0	10
34 <sub>r</sub>	0	2	12	4	10	4	0	4	12	0	2	4	2	2	2	4
35 <sub>r</sub>	6	4	4	0	10	0	0	4	10	0	0	4	2	8	8	4
36 <sub>r</sub>	4	6	2	2	2	6	8	6	4	2	6	0	4	10	0	0
37 <sub>r</sub>	2	2	8	2	4	4	4	2	6	2	0	10	6	10	2	0
38 <sub>r</sub>	0	4	8	4	2	6	6	2	4	2	2	4	6	4	4	6
39 <sub>r</sub>	4	4	4	8	0	6	0	6	4	8	2	2	2	4	8	2
3A <sub>r</sub>	8	8	0	4	2	0	10	4	0	0	0	4	8	6	8	2
3B <sub>r</sub>	8	2	6	4	4	4	4	0	6	4	4	6	4	4	4	0
3C <sub>r</sub>	0	6	6	6	0	0	8	8	2	4	8	4	2	4	0	0
3D <sub>r</sub>	2	2	8	10	0	2	12	0	4	0	8	0	2	2	4	8
3E <sub>r</sub>	6	4	0	0	4	4	0	10	6	2	6	12	2	4	0	4
3F <sub>r</sub>	0	6	6	0	4	4	6	10	0	6	8	2	0	4	8	0