

### Appendix - The Difference Distribution Tables

### The Difference Distribution Table of S1

Input XOR	Output XOR															
	$0_1$	$1_1$	$2_1$	$3_1$	$4_1$	$5_1$	$6_1$	$7_1$	$8_1$	$9_1$	$A_1$	$B_1$	$C_1$	$D_1$	$E_1$	$F_1$
$0_1$	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$1_1$	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
$2_1$	0	0	0	8	0	4	4	0	6	8	6	12	6	4	2	8
$3_1$	14	4	2	2	10	6	2	0	4	4	0	2	6	4	0	2
$4_1$	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
$5_1$	0	0	0	2	2	4	4	0	2	4	0	12	2	4	6	0
$6_1$	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
$7_1$	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
$8_1$	0	0	0	12	0	8	8	4	0	8	4	6	2	8	8	0
$9_1$	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	2
$A_1$	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
$B_1$	2	4	0	10	2	2	10	0	2	6	2	6	2	6	4	2
$C_1$	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
$D_1$	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
$E_1$	0	4	8	16	2	4	0	6	0	4	0	6	4	0	0	8
$F_1$	2	0	2	4	4	6	4	2	4	8	2	2	2	2	6	8
$10_1$	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
$11_1$	6	8	2	4	6	8	6	4	0	6	6	0	4	0	0	0
$12_1$	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0
$13_1$	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
$14_1$	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
$15_1$	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
$16_1$	0	8	10	8	0	2	2	6	10	2	2	0	2	0	6	6
$17_1$	4	4	6	4	2	4	0	2	4	0	2	4	4	6	4	4
$18_1$	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
$19_1$	2	6	2	4	0	4	8	6	10	4	0	4	2	8	4	0
$1A_1$	0	6	4	0	4	6	6	6	2	2	0	4	4	6	6	8
$1B_1$	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2
$1C_1$	0	10	4	6	6	0	0	12	6	4	0	0	2	6	14	0
$1D_1$	4	2	4	0	8	0	2	10	0	2	10	0	4	0	4	0
$1E_1$	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
$1F_1$	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																
	$0_1$	$1_1$	$2_1$	$3_1$	$4_1$	$5_1$	$6_1$	$7_1$	$8_1$	$9_1$	$A_1$	$B_1$	$C_1$	$D_1$	$E_1$	$F_1$	
$20_1$	0	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12
$21_1$	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8	8
$22_1$	10	4	6	8	2	2	2	6	2	6	0	2	4	10	2	6	6
$23_1$	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10	4
$24_1$	12	0	0	2	2	2	0	14	14	2	0	2	0	6	2	2	0
$25_1$	6	4	4	12	4	4	10	2	2	2	0	4	2	2	2	2	0
$26_1$	0	0	0	4	10	10	2	4	0	4	6	4	4	4	2	0	0
$27_1$	10	4	2	8	0	2	4	8	0	4	8	8	4	4	0	2	2
$28_1$	12	2	2	8	2	6	12	0	0	2	6	0	4	0	0	2	2
$29_1$	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4	0
$30_1$	4	2	4	8	0	2	2	14	2	6	2	6	2	6	2	2	2
$31_1$	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4	0
$32_1$	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6	0
$33_1$	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4	0
$34_1$	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6	6
$35_1$	2	2	2	4	0	8	0	0	14	4	6	8	0	2	14	0	0
$36_1$	0	6	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$37_1$	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4	4
$38_1$	0	6	2	2	2	2	0	2	2	4	6	4	4	6	10	10	0
$39_1$	6	2	2	2	2	2	4	8	4	0	2	4	4	4	4	0	0
$3A_1$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	4	0
$3B_1$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2	2
$3C_1$	0	10	0	0	12	6	4	8	4	0	2	4	0	12	4	4	0
$3D_1$	0	8	6	2	2	0	8	4	4	0	4	0	12	4	4	4	0
$3E_1$	4	8	2	2	4	0	14	4	2	4	0	0	8	4	0	4	0
$3F_1$	4	8	4	2	2	4	0	2	4	2	4	8	8	6	2	2	2

### The Difference Distribution Table of S2

Input XOR	Output XOR																		
	$0_1$	$1_1$	$2_1$	$3_1$	$4_1$	$5_1$	$6_1$	$7_1$	$8_1$	$9_1$	$A_1$	$B_1$	$C_1$	$D_1$	$E_1$	$F_1$			
$0_1$	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
$1_1$	0	0	0	0	0	2	6	4	0	4	0	4	0	4	6	2	6		
$2_1$	0	0	0	2	0	2	0	8	0	4	12	10	4	6	8	8			
$3_1$	4	8	4	8	4	8	6	0	6	4	2	2	2	4	6	2	4		
$4_1$	0	0	0	2	0	6	0	14	0	6	10	6	10	6	4	4	0		
$5_1$	6	2	4	8	6	10	6	10	6	2	8	2	0	2	0	4	2		
$6_1$	0	12	6	4	6	4	6	4	6	2	2	10	2	8	2	0	0		
$7_1$	4	6	6	4	2	4	2	4	2	4	2	4	2	4	6	0	0		
$8_1$	0	0	0	0	0	0	0	0	0	0	0	16	6	0	0	0	0		
$9_1$	14	2	4	10	2	8	2	6	2	4	0	0	0	2	2	2	4		
$A_1$	8	6	4	2	4	0	2	2	10	2	10	2	0	2	4	4	8		
$B_1$	6	2	2	2	0	2	4	6	2	10	2	0	6	6	4	4	8		
$C_1$	0	0	0	4	0	14	0	10	0	0	6	2	4	4	8	6	6		
$D_1$	0	6	12	8	0	4	2	2	0	8	2	4	4	6	2	0	6		
$E_1$	0	8	2	0	6	6	8	2	4	4	4	4	6	8	0	4	2		
$F_1$	0	8	2	0	6	6	8	2	4	4	4	4	6	8	0	4	2		
$10_1$	4	0	4	0	8	6	6	0	0	2	2	0	6	4	10	6	4		
$11_1$	6	6	4	6	4	0	6	6	0	6	4	8	2	10	2	4	0	0	
$12_1$	0	6	2	6	2	4	12	4	6	4	0	4	0	4	6	2	2	2	
$13_1$	4	0	4	0	8	6	6	0	0	2	2	0	6	4	10	2	14	0	
$14_1$	0	6	6	4	10	0	2	12	6	2	2	2	2	4	4	2	2	2	
$15_1$	6	8	2	0	8	2	0	2	2	2	2	2	2	2	14	10	2	2	
$16_1$	6	4	8	6	4	2	4	0	4	6	2	4	4	4	2	4	2	2	
$17_1$	0	6	4	6	10	4	0	2	2	4	8	0	0	4	4	8	2	6	6
$18_1$	0	6	4	6	10	4	0	2	2	4	8	0	0	4	4	8	2	6	6
$19_1$	0	6	8	4	2	4	2	2	8	2	2	2	2	2	4	4	8	8	
$1A_1$	0	6	4	4	0	12	6	4	4	2	2	2	2	4	4	2	10	2	2
$1B_1$	0	6	4	4	0	12	6	4	4	2	2	2	2	4	4	2	10	2	2
$1C_1$	0	6	2	2	6	0	4	16	4	4	2	0	0	4	2	0	6	8	8
$1D_1$	0	6	2	2	6	0	6	0	0	4	2	0	0	4	4	0	6	8	8
$1E_1$	0	4	2	2	10	6	6	0	0	4	0	4	0	4	4	0	6	6	6
$1F_1$	4	2	6	6	2	2	2	4	8	6	10	6	6	4	0	0	2	2	2



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

Input MOR	Output XOR															
	$0_x$	$1_x$	$2_x$	$3_x$	$4_x$	$5_x$	$6_x$	$7_x$	$8_x$	$9_x$	$A_x$	$B_x$	$C_x$	$D_x$	$E_x$	$F_x$
20 <sub>x</sub>	0	0	0	10	0	4	0	0	0	14	6	4	2	0	4	11
21 <sub>x</sub>	0	0	2	10	2	8	10	0	0	6	6	0	10	2	2	6
22 <sub>x</sub>	8	0	6	0	6	4	10	2	0	6	8	0	4	4	2	4
23 <sub>x</sub>	4	8	0	6	0	4	8	6	2	2	10	4	8	0	0	2
24 <sub>x</sub>	4	0	4	8	4	6	2	4	8	6	2	0	0	4	4	8
25 <sub>x</sub>	0	4	6	8	2	8	8	0	4	2	4	4	2	2	6	4
26 <sub>x</sub>	2	6	0	6	4	4	4	6	6	0	4	4	10	4	2	2
27 <sub>x</sub>	6	6	0	0	2	2	6	2	4	4	6	10	2	6	2	6
28 <sub>x</sub>	10	2	6	2	4	12	12	0	2	2	4	0	0	0	2	6
29 <sub>x</sub>	4	0	0	14	2	10	4	2	8	6	4	0	0	4	2	2
2A <sub>x</sub>	8	8	0	2	0	2	4	0	2	6	8	14	2	8	0	0
2B <sub>x</sub>	2	2	0	0	4	2	10	4	6	2	4	0	6	4	8	10
2C <sub>x</sub>	2	6	6	2	4	6	2	0	2	6	4	0	6	4	10	4
2D <sub>x</sub>	8	0	4	4	6	2	0	0	6	8	2	4	6	4	4	6
2E <sub>x</sub>	6	2	2	4	2	2	6	12	4	0	4	2	8	8	0	2
2F <sub>x</sub>	8	12	4	6	6	4	2	2	2	2	4	2	2	4	0	4
30 <sub>x</sub>	0	4	6	2	10	2	2	2	4	8	0	0	8	4	6	6
31 <sub>x</sub>	4	6	8	0	4	6	0	4	6	10	2	2	4	4	0	0
32 <sub>x</sub>	6	6	6	2	4	6	0	2	0	6	8	2	2	6	6	2
33 <sub>x</sub>	6	6	4	2	4	0	0	10	2	2	0	6	8	4	0	10
34 <sub>x</sub>	0	2	12	4	10	4	0	4	12	0	2	4	2	2	2	4
35 <sub>x</sub>	6	4	4	0	10	0	0	4	10	0	0	4	2	8	8	4
36 <sub>x</sub>	4	6	2	2	2	6	8	6	4	2	6	0	4	10	0	0
37 <sub>x</sub>	2	2	8	2	4	4	4	2	6	2	0	10	6	10	2	0
38 <sub>x</sub>	0	4	8	4	2	6	6	2	4	2	2	4	6	4	4	6
39 <sub>x</sub>	4	4	4	8	0	6	0	6	4	8	2	2	2	4	8	2
3A <sub>x</sub>	8	8	0	4	2	0	10	4	0	0	0	4	8	6	8	2
3B <sub>x</sub>	8	2	6	4	4	4	4	0	6	4	4	6	4	4	4	0
3C <sub>x</sub>	0	6	6	6	6	0	0	8	8	2	4	8	4	2	4	0
3D <sub>x</sub>	2	2	8	0	10	0	2	12	0	4	0	8	0	2	6	8
3E <sub>x</sub>	6	4	0	0	4	4	0	10	6	2	6	12	2	4	0	4
3F <sub>x</sub>	0	6	6	0	4	4	6	10	0	6	8	2	0	4	8	0