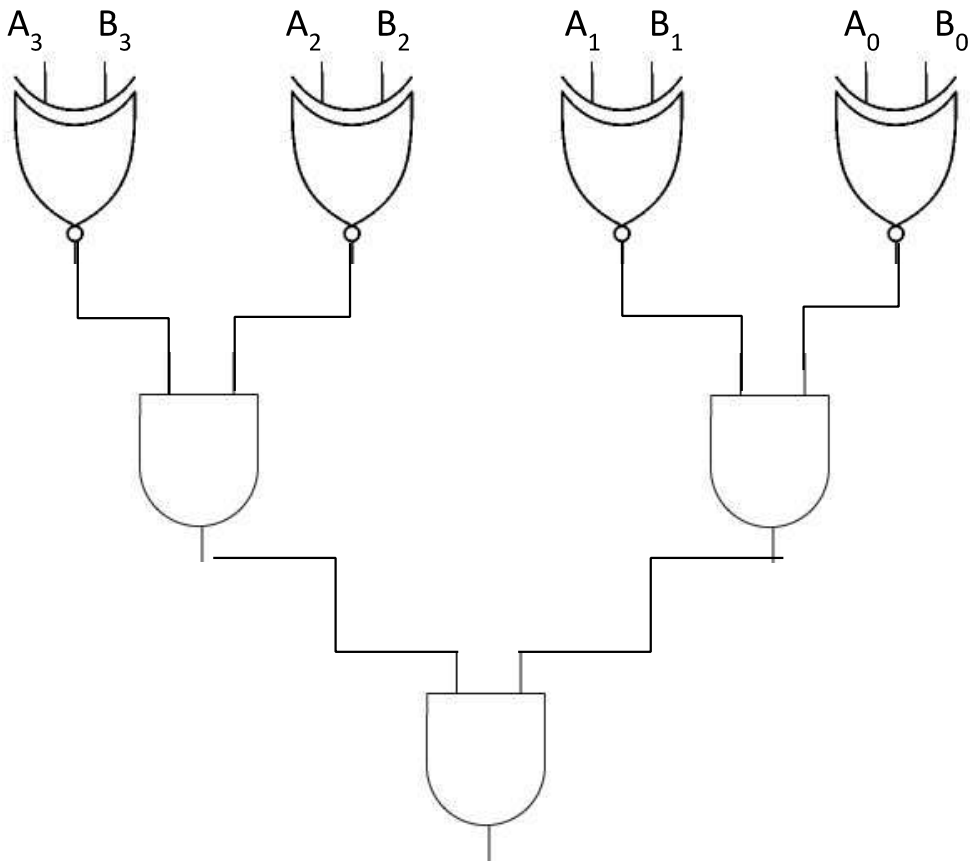
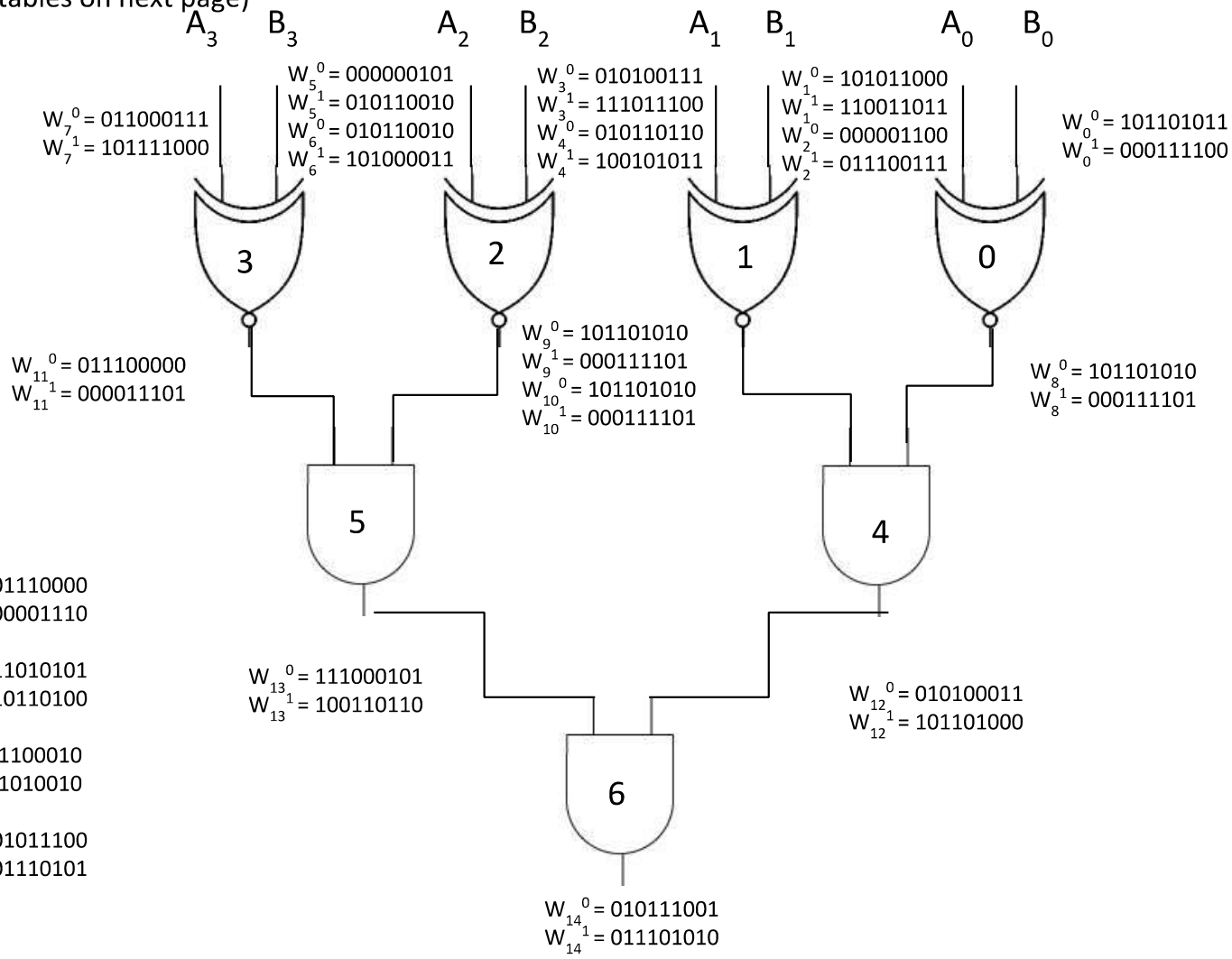
Original Circuit(let a denote alice's input and b bob's)



- Garbled Circuit(Truth tables on next page)



V_{10}^0 =10110101
V_{10}^1 =00011110
p_{10} = 1
V_9^0 =10110101
V_9^1 =00011110
p_9 = 1
V_8^0 =10110101
V_8^1 =00011110
p_8 = 1
V_7^0 = 01100011
V_7^1 = 10111100
p_7 = 1
V_6^0 = 01011001
V_6^1 = 10100001
p_6 = 0
V_5^0 =00000010
V_5^1 =01011001
p_5 = 1
V_4^0 = 01011011
V_4^1 = 10010101
p_4 = 0
V_3^0 = 01010011
V_3^1 = 11101110
p_3 = 1
V_2^0 = 00000110
V_2^1 = 01110011
p_2 = 0
V_1^0 = 10101100
V_1^1 =11001101
p_1 = 0
V_0^0 =10110101
V_0^1 =00011110
p_0 = 1

V_{11}^0 = 01110000
V_{11}^1 = 00001110
p_{11} = 1
V_{12}^0 = 11010101
V_{12}^1 = 10110100
p_{12} = 0
V_{13}^0 =11100010
V_{13}^1 =11010010
p_{13} = 0
V_{14}^0 = 01011100
V_{14}^1 = 01110101
p_{14} = 0

0

x	y	out	Encrypt	x	y	out	Shuffle	X	y	out
W_1^0	W_0^0	W_8^1	$E\,V_1^0\,V_0^0\,001$	W_1^0	W_0^0	W_8^1	$E\,V_1^0\,V_0^1\,000$	W_1^0	W_0^1	W_8^0
W_1^0	W_0^1	W_8^0	$E\,V_1^0\,V_0^1\,000$	W_1^0	W_0^1	W_8^0	$E\,V_1^0\,V_0^0\,001$	W_1^0	W_0^0	W_8^1
W_1^1	W_0^0	W_8^0	$E\,V_1^1\,V_0^0\,011$	W_1^1	W_0^0	W_8^0	$E\,V_1^1\,V_0^1\,010$	W_1^1	W_0^1	W_8^1
W_1^1	W_0^1	W_8^1	$E\,V_1^1\,V_0^1\,010$	W_1^1	W_0^1	W_8^1	$E\,V_1^1\,V_0^0\,011$	W_1^1	W_0^0	W_8^0

1

x	y	out	Encrypt	x	y	out	Shuffle	X	y	out
W_3^0	W_2^0	W_9^1	$E\,V_3^0\,V_2^0\,110$	W_3^0	W_2^0	W_9^1	$E\,V_3^0\,V_2^0\,110$	W_3^1	W_2^0	W_9^0
W_3^0	W_2^1	W_9^0	$E\,V_3^0\,V_2^0\,111$	W_3^0	W_2^1	W_9^0	$E\,V_3^0\,V_2^0\,101$	W_3^1	W_2^1	W_9^1
W_3^1	W_2^0	W_9^0	$E\,V_3^0\,V_2^0\,100$	W_3^1	W_2^0	W_9^0	$E\,V_3^0\,V_2^0\,110$	W_3^0	W_2^0	W_9^1
W_3^1	W_2^1	W_9^1	$E\,V_3^0\,V_2^0\,101$	W_3^1	W_2^1	W_9^1	$E\,V_3^0\,V_2^0\,101$	W_3^0	W_2^1	W_9^0

2

x	y	out	Encrypt	x	y	out	Shuffle	X	y	out
W_5^0	W_4^0	W_{10}^1	$E\,V_5^0\,V_4^0\,210$	W_5^0	W_4^0	W_{10}^1	$E\,V_5^1\,V_4^0\,200$	W_5^1	W_4^0	W_{10}^0
W_5^0	W_4^1	W_{10}^0	$E\,V_5^0\,V_4^1\,211$	W_5^0	W_4^1	W_{10}^0	$E\,V_5^1\,V_4^1\,201$	W_5^1	W_4^1	W_{10}^1
W_5^1	W_4^0	W_{10}^0	$E\,V_5^1\,V_4^0\,200$	W_5^1	W_4^0	W_{10}^0	$E\,V_5^0\,V_4^0\,210$	W_5^0	W_4^0	W_{10}^1
W_5^1	W_4^1	W_{10}^1	$E\,V_5^1\,V_4^1\,201$	W_5^1	W_4^1	W_{10}^1	$E\,V_5^0\,V_4^1\,211$	W_5^0	W_4^1	W_{10}^0

3

x	y	out
W_7^0	W_6^0	W_{11}^1
W_7^0	W_6^1	W_{11}^0
W_7^1	W_6^0	W_{11}^0
W_7^1	W_6^1	W_{11}^1

Encrypt

$E\,V_7^0\,V_6^0\,310$

$E\,V_7^0\,V_6^1\,311$

$E\,V_7^1\,V_6^0\,300$

$E\,V_7^1\,V_6^1\,301$

x	y	out
W_7^0	W_6^0	W_{11}^1
W_7^0	W_6^1	W_{11}^0
W_7^1	W_6^0	W_{11}^0
W_7^1	W_6^1	W_{11}^1

Shuffle

$E\,V_7^1\,V_6^0\,300$

$E\,V_7^1\,V_6^1\,301$

$E\,V_7^0\,V_6^0\,310$

$E\,V_7^0\,V_6^1\,311$

x	y	out
W_7^1	W_6^0	W_{11}^0
W_7^1	W_6^1	W_{11}^1
W_7^0	W_6^0	W_{11}^1
W_7^0	W_6^1	W_{11}^0

4

x	y	out
W_9^0	W_8^0	W_{12}^0
W_9^0	W_8^1	W_{12}^0
W_9^1	W_8^0	W_{12}^0
W_9^1	W_8^1	W_{12}^1

Encrypt

$E\,V_9^0\,V_8^0\,411$

$E\,V_9^0\,V_8^1\,410$

$E\,V_9^1\,V_8^0\,401$

$E\,V_9^1\,V_8^1\,400$

x	y	out
W_9^0	W_8^0	W_{12}^0
W_9^0	W_8^1	W_{12}^0
W_9^1	W_8^0	W_{12}^0
W_9^1	W_8^1	W_{12}^1

Shuffle

$E\,V_9^1\,V_8^1\,400$

$E\,V_9^1\,V_8^0\,401$

$E\,V_9^0\,V_8^1\,410$

$E\,V_9^0\,V_8^0\,411$

x	y	out
W_9^1	W_8^1	W_{12}^1
W_9^1	W_8^0	W_{12}^0
W_9^0	W_8^1	W_{12}^0
W_9^0	W_8^0	W_{12}^0

5

x	y	out
W_{11}^0	W_{10}^0	W_{13}^0
W_{11}^0	W_{10}^1	W_{13}^0
W_{11}^1	W_{10}^0	W_{13}^0
W_{11}^1	W_{10}^1	W_{13}^1

Encrypt

$E\,V_{11}^0\,V_{10}^0\,511$

$E\,V_{11}^0\,V_{10}^1\,510$

$E\,V_{11}^1\,V_{10}^0\,501$

$E\,V_{11}^1\,V_{10}^1\,500$

x	y	out
W_{11}^0	W_{10}^0	W_{13}^0
W_{11}^0	W_{10}^1	W_{13}^0
W_{11}^1	W_{10}^0	W_{13}^0
W_{11}^1	W_{10}^1	W_{13}^1

Shuffle

$E\,V_{11}^1\,V_{10}^1\,500$

$E\,V_{11}^1\,V_{10}^0\,501$

$E\,V_{11}^0\,V_{10}^1\,510$

$E\,V_{11}^0\,V_{10}^0\,511$

x	y	out
W_{11}^1	W_{10}^1	W_{13}^1
W_{11}^0	W_{10}^1	W_{13}^0
W_{11}^0	W_{10}^1	W_{13}^0
W_{11}^0	W_{10}^0	W_{13}^0

6

x	y	out
W_{13}^{0}	W_{12}^{0}	W_{14}^{0}
W_{13}^{0}	W_{12}^{1}	W_{14}^{0}
W_{13}^{1}	W_{12}^{0}	W_{14}^{0}
W_{13}^{1}	W_{12}^{1}	W_{14}^{1}

Encrypt →

x	y	out
W_{13}^{0}	W_{12}^{0}	W_{14}^{0}
W_{13}^{0}	W_{12}^{1}	W_{14}^{0}
W_{13}^{1}	W_{12}^{0}	W_{14}^{0}
W_{13}^{1}	W_{12}^{1}	W_{14}^{1}

$E\,V_{13}^{0}\,V_{12}^{0}\,600$

$E\,V_{13}^{0}\,V_{12}^{1}\,601$

$E\,V_{13}^{1}\,V_{12}^{0}\,610$

$E\,V_{13}^{1}\,V_{12}^{1}\,611$

Shuffle →

x	y	out
W_{13}^{0}	W_{12}^{0}	W_{14}^{0}
W_{13}^{0}	W_{12}^{1}	W_{14}^{0}
W_{13}^{1}	W_{12}^{0}	W_{14}^{0}
W_{13}^{1}	W_{12}^{1}	W_{14}^{1}

$E\,V_{13}^{0}\,V_{12}^{0}\,600$

$E\,V_{13}^{0}\,V_{12}^{1}\,601$

$E\,V_{13}^{1}\,V_{12}^{0}\,610$

$E\,V_{13}^{1}\,V_{12}^{1}\,611$