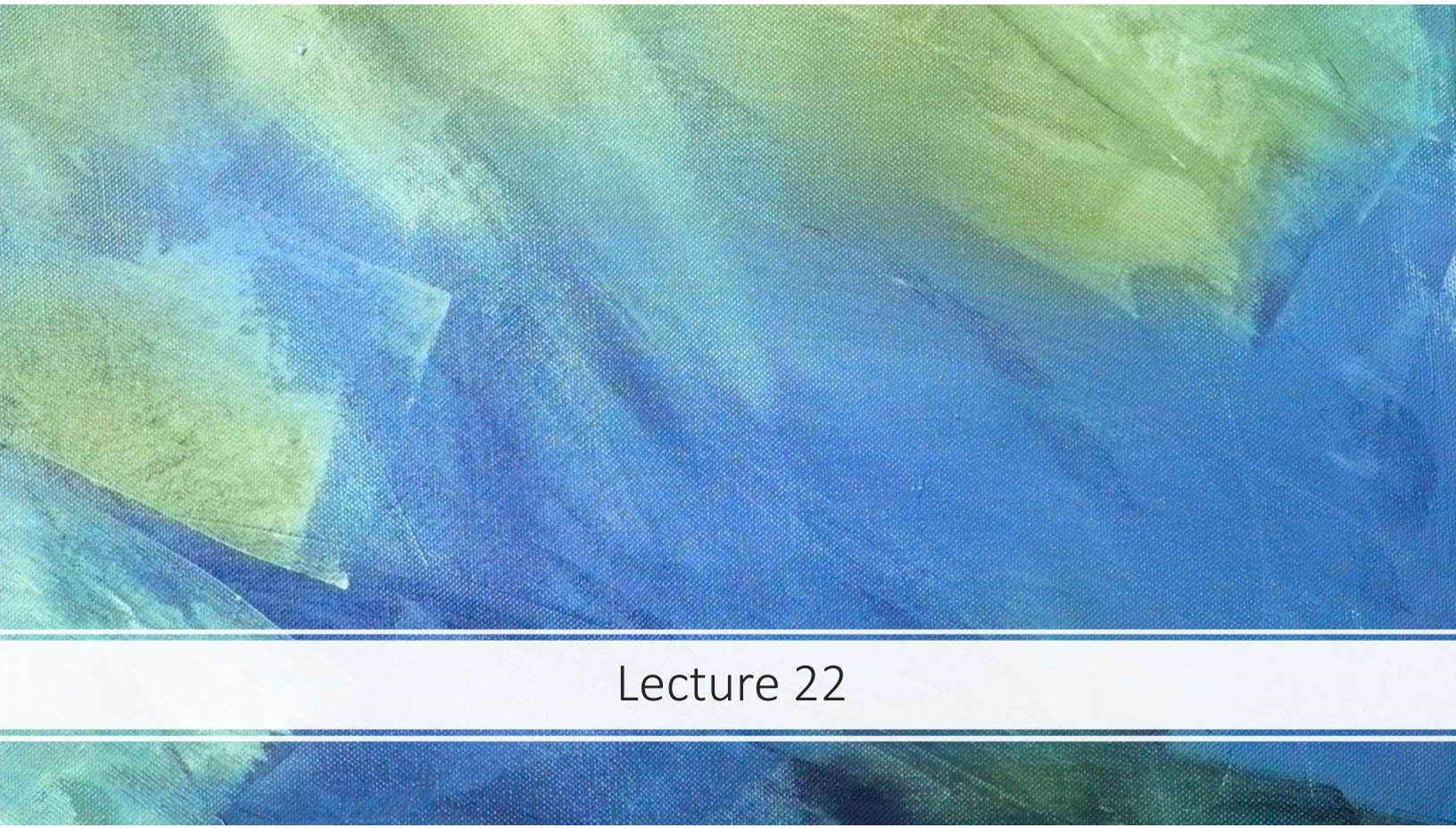
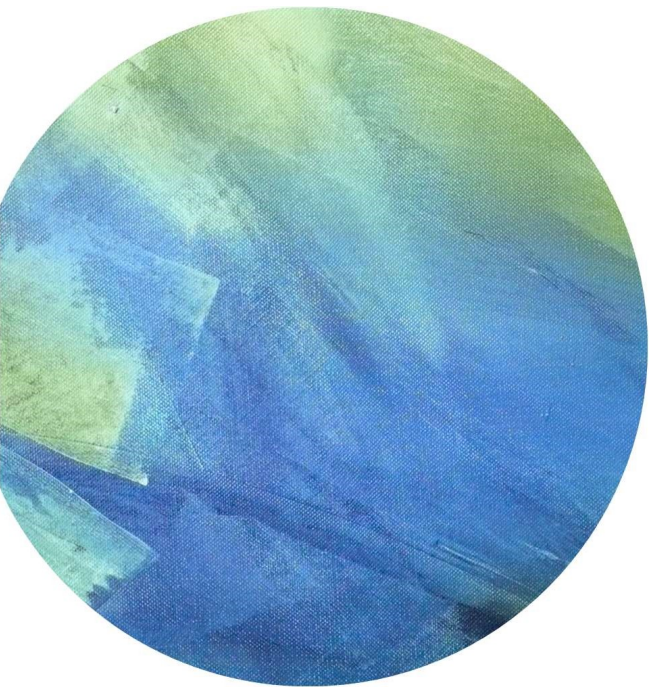

Lecture 22

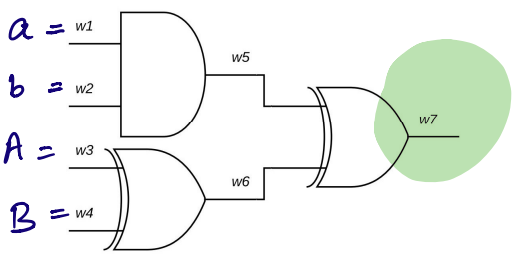


Outline

Secure Computation

Garbled Circuits

Computing General Circuits on Private Inputs



a_0
A_0
b_0
B_0

a, A

$\Downarrow$

$a_0, a_1 \leftarrow \{0,1\} \times \{0,1\}$

s.t. $a_0 \oplus a_1 = a$.

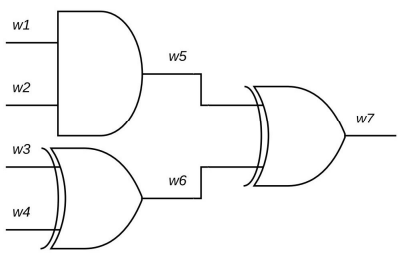
a_1
A_1
b_1
B_1

b, B

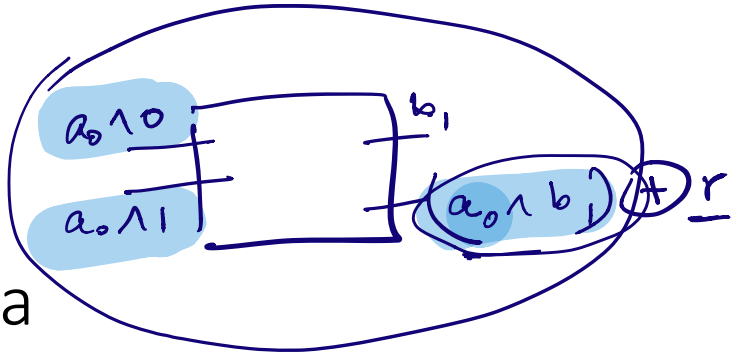
$\downarrow$ $\qquad$ $\searrow$

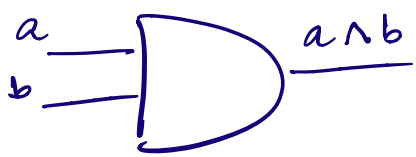
b_0, b_1 $\qquad$ B_0, B_1

General circuits on Shared Data



AND on secret-shared data





a_1

$a_1 \wedge b_0$

a

a_1
b_1

(a_1, b_1)

b_0

$b \rightarrow b_0 = b \oplus b_1$

$$(a \wedge b) = (a_0 \oplus a_1) \wedge (b_0 \oplus b_1)$$

$$= \underbrace{(a_0 \wedge b_0)}_{\text{Alice}} \oplus \underbrace{(a_0 \wedge b_1)}_{\text{Bob}} \oplus \underbrace{(a_1 \wedge b_0)}_{\text{Alice}} \oplus \underbrace{(a_1 \wedge b_1)}_{\text{Bob}}$$

Bob knows: $(a_0 \wedge b_1) \oplus (a_1 \wedge b_1) \rightarrow (a_0 \oplus a_1) \wedge b_1$

$= (a \wedge b_1)$

AND on secret-shared data

a

$b_0, b_1 \xleftarrow{\text{unif.}} \{0,1\} \times \{0,1\}$

Recall: $b_0 \oplus b_1 = b$.

$b = 0$

Bob's output: 0

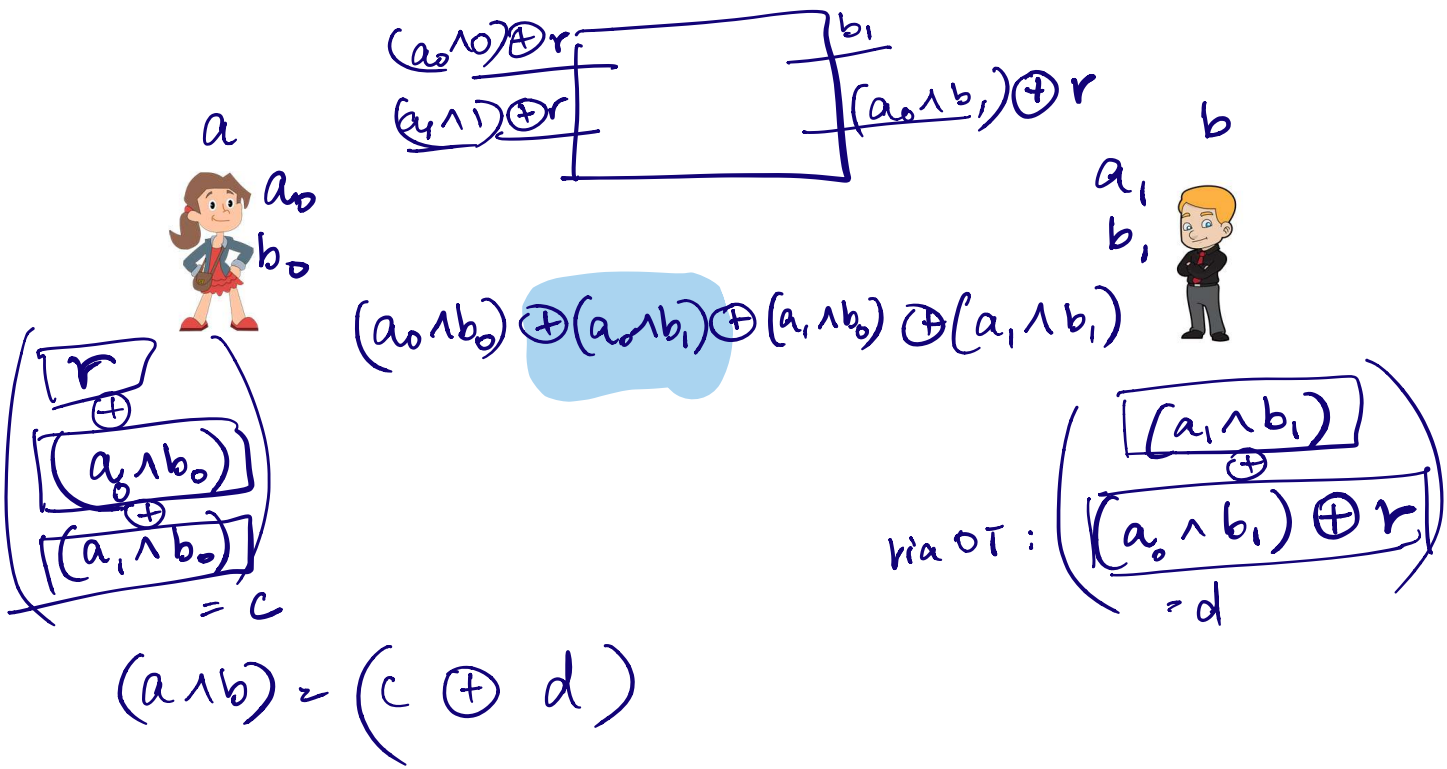
Bob recovers $a \wedge b_1$

What if $b_1 = 1$?

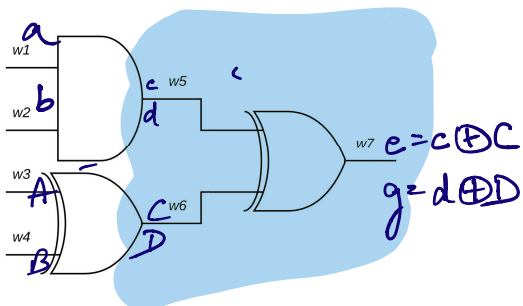
(happens w.p. $\frac{1}{2}$)

Then $a \wedge b_1 = a \wedge 1 = a$.

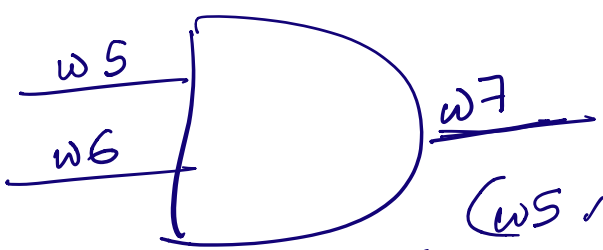
AND on secret-shared data



Computing General Circuits on Private Inputs



Alice has c,
Bob has d s.t.
w5 = c⊕d

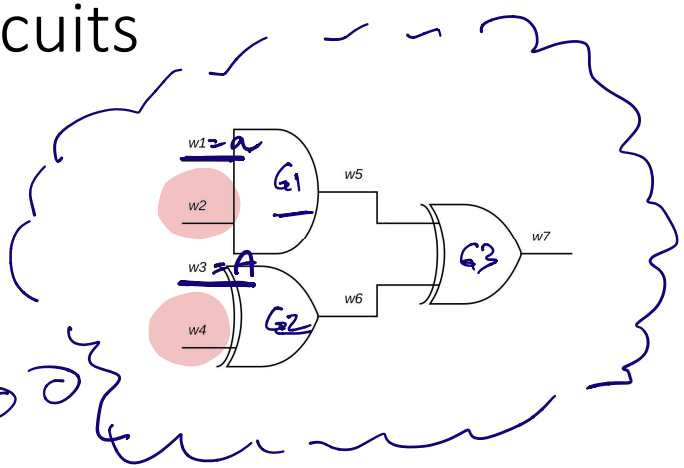


(w5 ∧ w6)
= (c⊕d) ∧ (C⊕D)

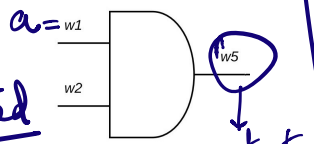
A Different Route: Garbled Circuits

Garbled Circuits

(Yao '86)



Garbled Gate



G. →

a ↓	b ↓	
w1	w2	w5
0	0	0
0	1	0
1	0	0
1	1	1

Authenticated Key for symmetric key encryption →

a

$K_{w1,0}$

$K_{w1,1}$

$K_{w2,0}$

$K_{w2,1}$

Garbled Table

$E_{K_{w1,0}}(E_{K_{w2,0}}(K_{w5,0}))$

$E_{K_{w1,0}}(E_{K_{w2,1}}(K_{w5,0}))$

$E_{K_{w1,1}}(E_{K_{w2,0}}(K_{w5,0}))$

$E_{K_{w1,1}}(E_{K_{w2,1}}(K_{w5,1}))$

to Bob →

randomize the rows.

$K_{w5,0}$

$K_{w5,1}$

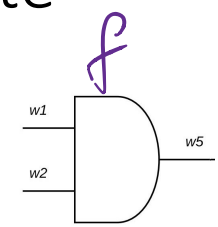
$K_{w5,0}$: 0

$K_{w5,1}$: 1

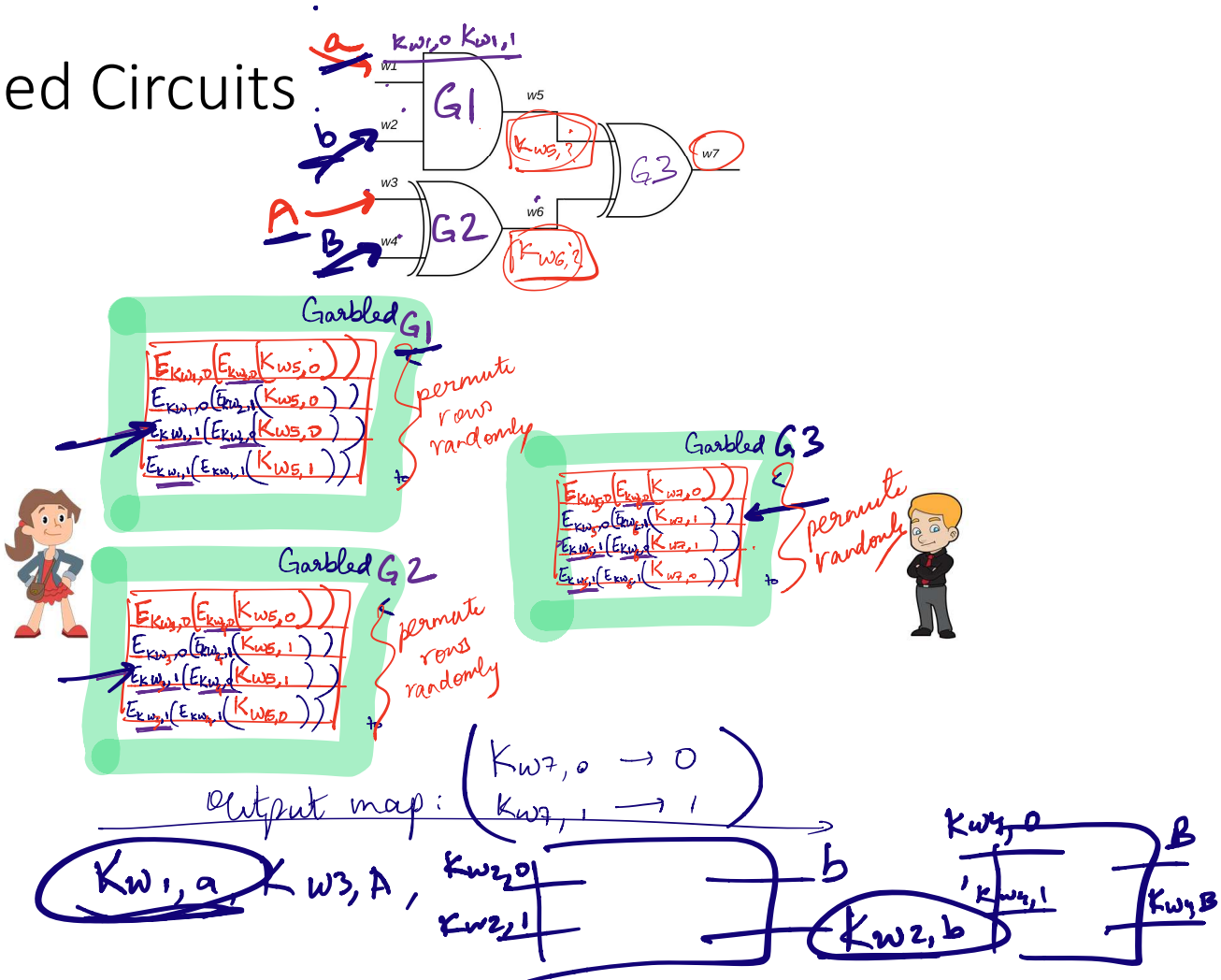
to Bob →

(K_{w1}, a) to Bob

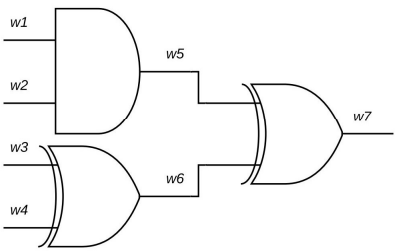
Garbled Gate



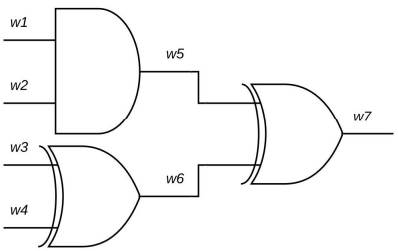
Garbled Circuits



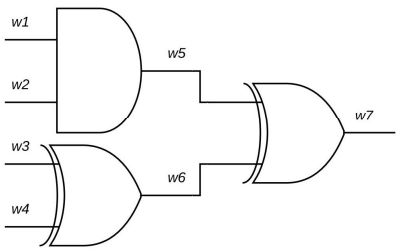
Garbled Circuits



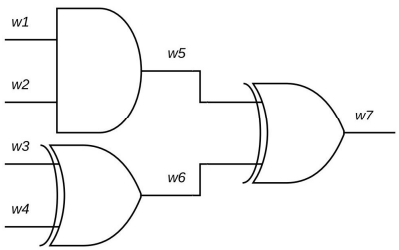
Garbled Circuits



Garbled Circuits + OT



Garbled Circuits + OT



Alice a — $f(a,b)$ — f — Bob b — $f(a,b)$