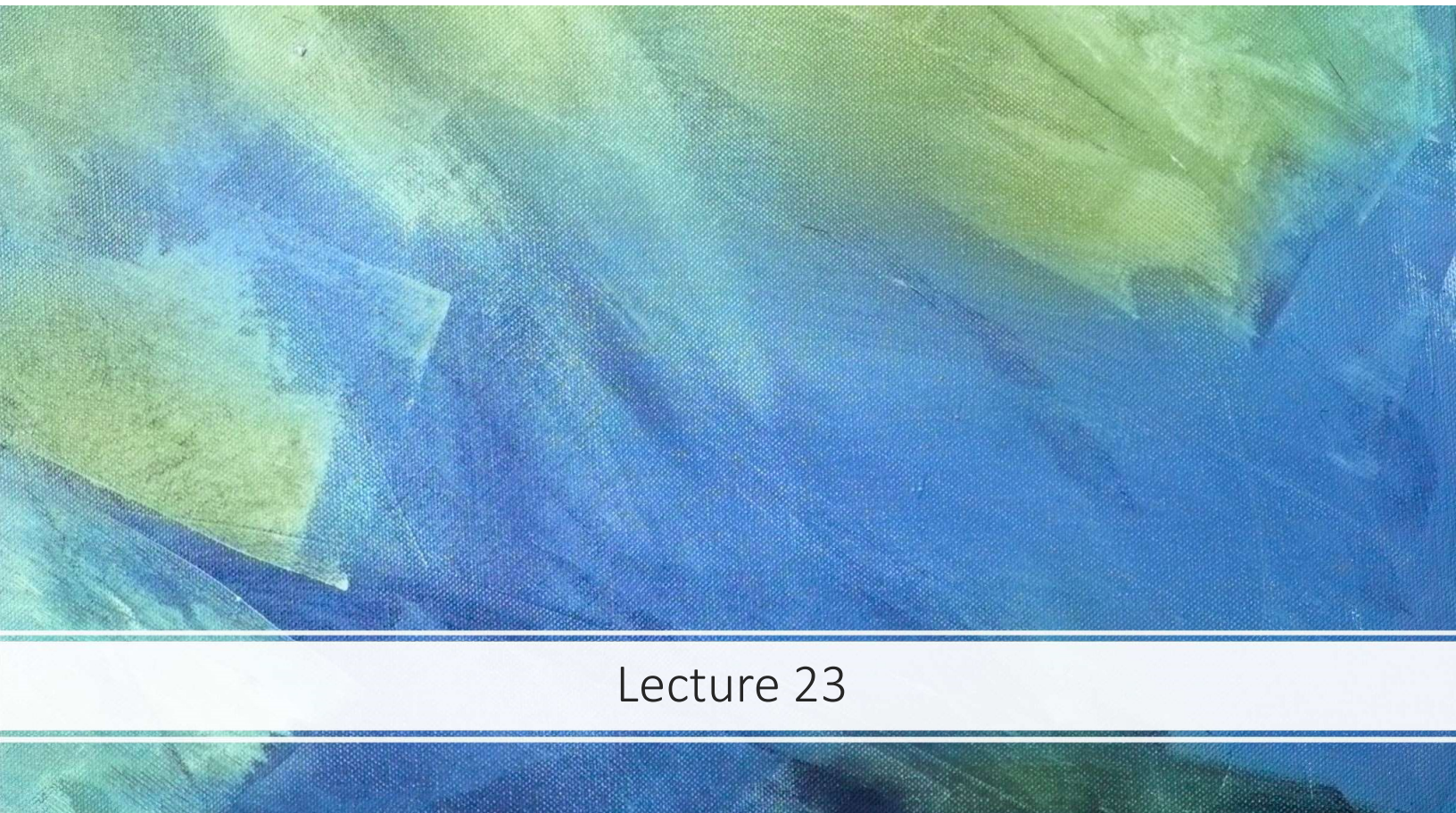
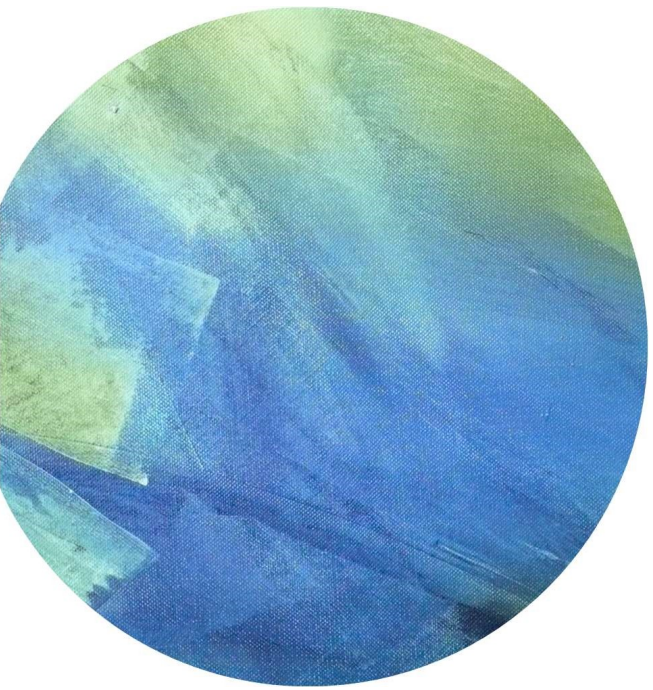

Lecture 23

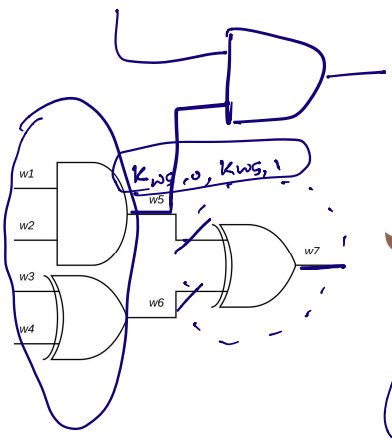


Outline

Garbled Circuits: Security

Q & A from Homework

Garbled Circuits: Security

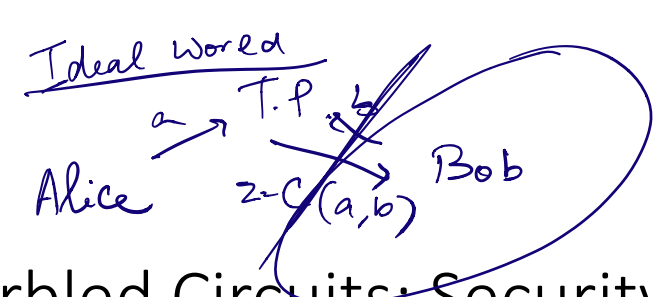


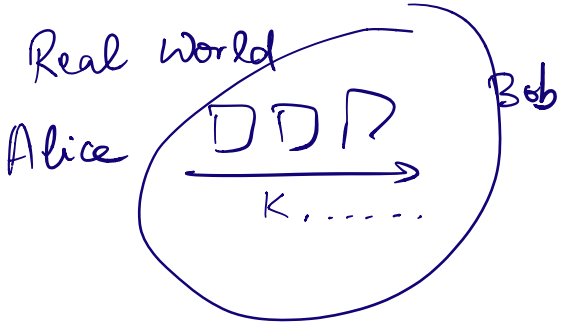
$K_{w5,0}, K_{w5,1}$

$(C, \vec{x})$

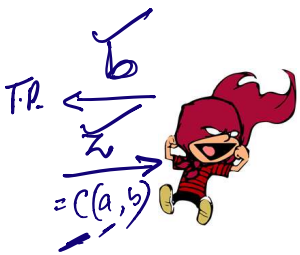
$Enc_{K_?}, Enc_{K_?}(K_?)$

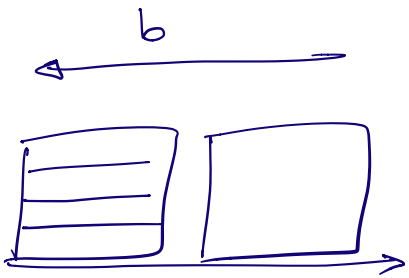
$C(a, b)$



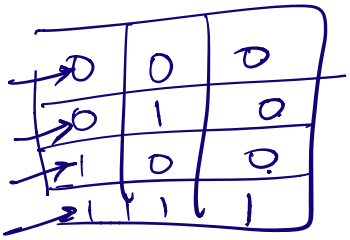


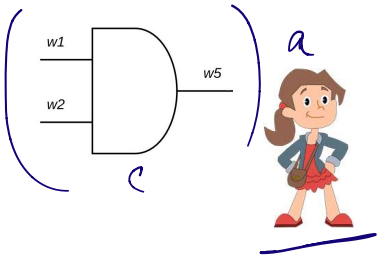
Garbled Circuits: Security

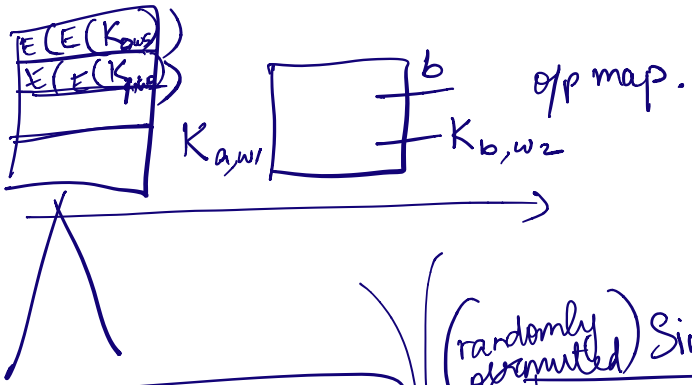


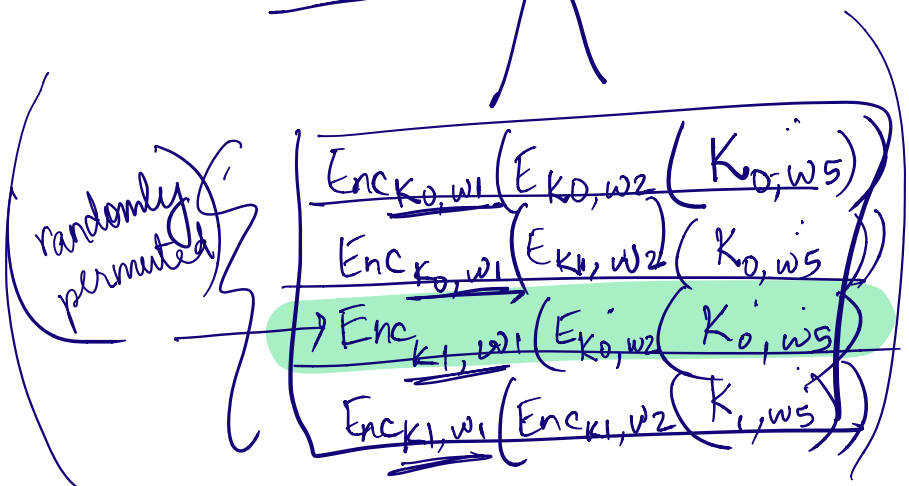


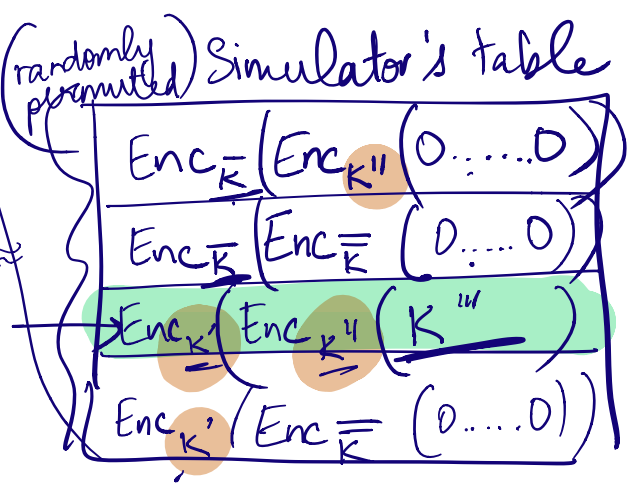
Garbled Gate

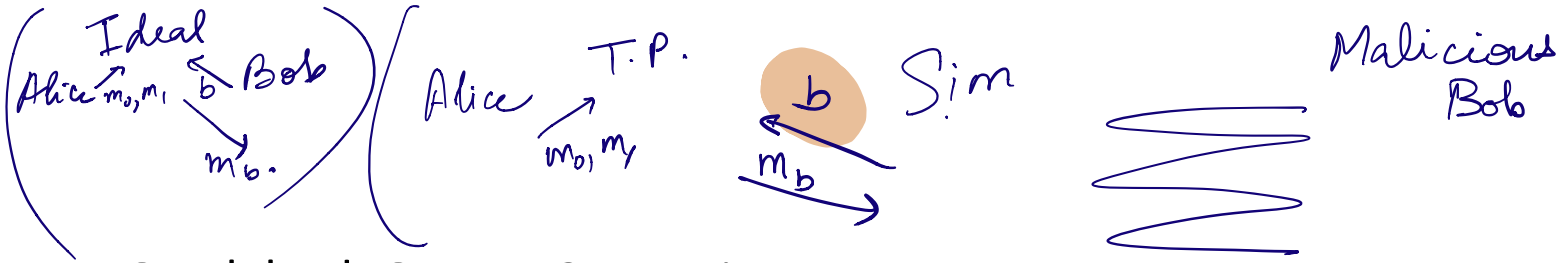




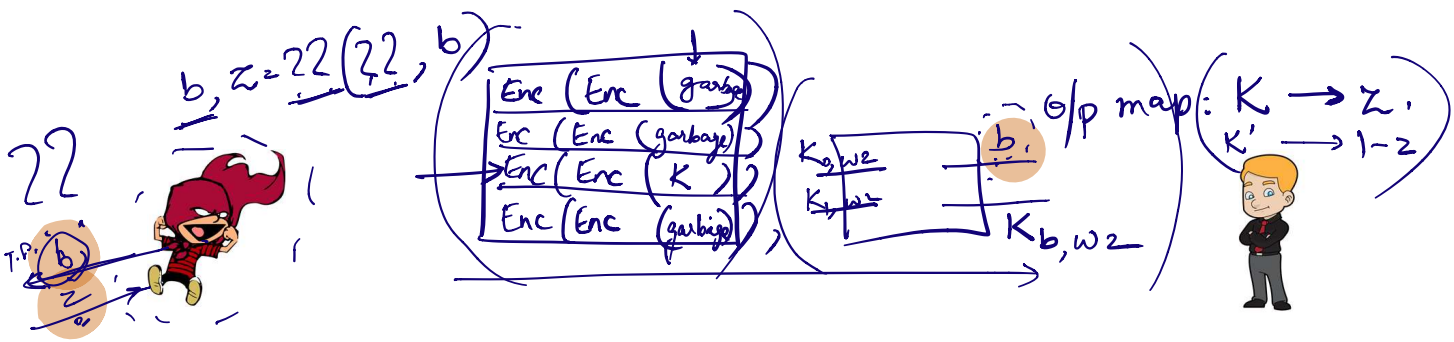








Garbled Gate: Security



Sim(b, z) : (Garbled Table G, Keys, output map)

where z = C(a, b)

AND.

k_a	k_b	K
0	0	0
0	1	0
1	0	0
1	1	1

permute

$E_{k_a,0}(E_{k_b,0}(K_0'))$

$E_{k_a,0}(E_{k_b,1}(K_0'))$

$E_{k_a,1}(E_{k_b,0}(K_0'))$

$E_{k_a,1}(E_{k_b,1}(K_1'))$

XOR

K_0

K_1

K_1

K_0

$=$

$E_{k_a,0}(E_{k_b,1}(K_0'))$

$E_{k_a,1}(E_{k_b,1}(K_1'))$

$E_{k_a,1}(E_{k_b,0}(K_0))$

$E_{k_a,0}(E_{k_b,0}(K_0))$

$K_0 \to 0$

$K_1 \to 1$.

$a = 0$

$\Rightarrow$ Send $K_{a,0}$.

Use OT to transmit 1 out of $K_{b,0}, K_{b,1}$ to Bob.

Bob's input $b = 1$ (w.l.o.g.)

Game 1 Same as Alice's interaction with Bob, except invoke OT simulator to learn Bob's input b, send $K_{b,1}$ to Sim.

Claim 1: Bob's view in interaction with Alice $\approx$ Bob's view in Game 1 [OT simulation security]

Game 2: Same as Game 1, except.

$E_{k_a,0}(E_{k_b,1}(K_0))$

$E_{k_a,1}(E_{k_b,1}(0 \ldots 0))$

$E_{k_a,1}(E_{k_b,0}(K_0))$

$E_{k_a,0}(E_{k_b,0}(K_0))$

Claim 2: Bob's view in Game 1 $\approx$ Bob's view in Game 2.

$\forall$ PPT $\mathcal{D}$,

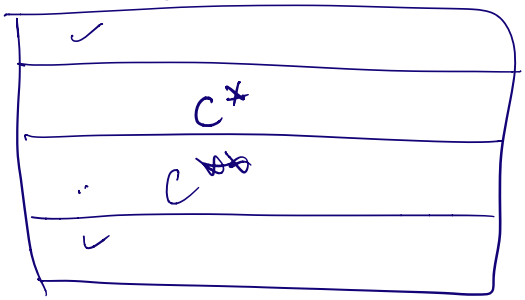
$$\left| \Pr[\mathcal{D}(\text{Game 1 view}) = 1] - \Pr[\mathcal{D}(\text{Game 2 view}) = 1] \right| = \text{negl}.$$

Proof: Suppose not. Then $\mathcal{W}$ that contradicts CPA-security of our encryption scheme.

$\mathcal{W}$ submits to CPA ch. $m_0 = E_{K_{b,1}}(K_1)$

$m_1 = E_{K_{b,1}}(0 \ldots 0)$

Obtains $c^* = E_{K_{a,1}}(m_d)$, $c^{**} = E_{K_{a,1}}(E_{K_{b,0}}(K_0))$



If $d = 0$, Game 1

$d = 1$, Game 2.

Game 3:

$E_{K_{a,0}}(E_{K_{b,1}}(K_0))$

$E_{K_{a,1}}(E_{K_{b,1}}(0 \ldots 0))$

$E_{K_{a,i}}(E_{K_{b,0}}(0 \ldots 0))$

$E_{K_{a,0}}(E_{K_{b,0}}(K_0))$

Bob obtains $K_{a,0}$, $K_{b,1}$.

Claim 3: Bob's view in Game 2 $\approx$ Bob's view in Game 3.

Game 4:

$E_{K_{a,0}}(E_{K_{b,1}}(K_0))$
$E_{K_{a,1}}(E_{K_{b,1}}(0\ldots0))$
$E_{K_{a,1}}(E_{K_{b,0}}(0\ldots0))$
$E_{K_{a,0}}(E_{K_{b,0}}(0\ldots0))$

$K_0 : 0$
$K_1 : 1$

Send $K_{a,0}$ $(K_{b,1})$ to Bob via OT sim.

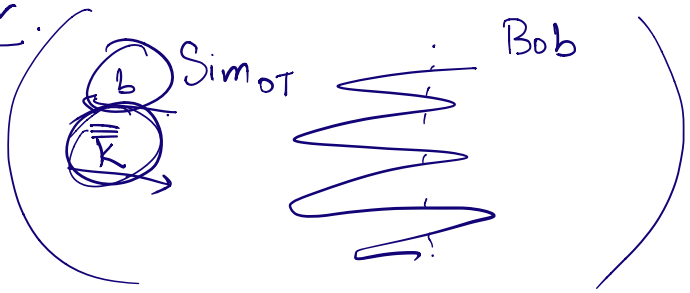
Claim 4: Bob's view in Game 3 $\approx$ Bob's view in Game 4.

Note: Game 4 is identical to Simulator's output upto renaming $K_{a,0} \to \bar{K}$

$K_{b,1} \to \bar{\bar{K}}$

$K_0 \to K_{out}$

Simulator



$b=1$,
$z=0$.

$E_{\tilde{K}}(E_{\bar{\bar{K}}}(0\ldots0))$
$E_{\tilde{K}}(E_{\bar{\bar{K}}}(K_{out}))$
$E_{K'}(E_{\bar{K}}(0\ldots0))$
$E_{K'}(E_{\bar{\bar{K}}}(0\ldots0))$

$(K_{out} \to 0,\ \tilde{K} \to 1)$

$(\bar{K}, \bar{\bar{K}})$