

The background of the slide is an abstract composition of broad, textured brushstrokes. The top half is dominated by various shades of green, ranging from a pale, almost white-green to a deep, forest green. The bottom half is primarily a rich, vibrant blue, with some darker, more muted tones interspersed. The brushstrokes are visible, giving the background a painterly, organic feel.

Lecture 28

Scribe : Fangqi

Outline

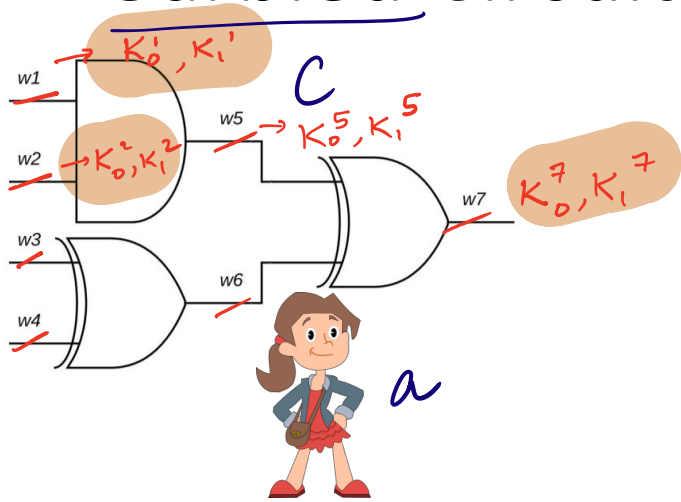


Garbled Circuits



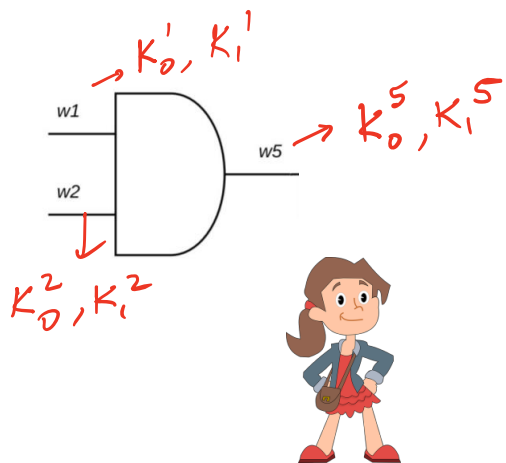
Security

Garbled Circuits



$C(a, b)$

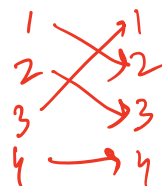
Garbled Gate



Garbled Table

w_1	w_2	w_5
0	0	0
0	1	0
1	0	0
1	1	1

randomly permuted



$\text{Enc}_{K_0^1}(\text{Enc}_{K_0^2}(K_0^5))$
$\text{Enc}_{K_0^1}(\text{Enc}_{K_1^2}(K_0^5))$
$\text{Enc}_{K_1^1}(\text{Enc}_{K_0^2}(K_1^5))$
$\text{Enc}_{K_1^1}(\text{Enc}_{K_1^2}(K_1^5))$

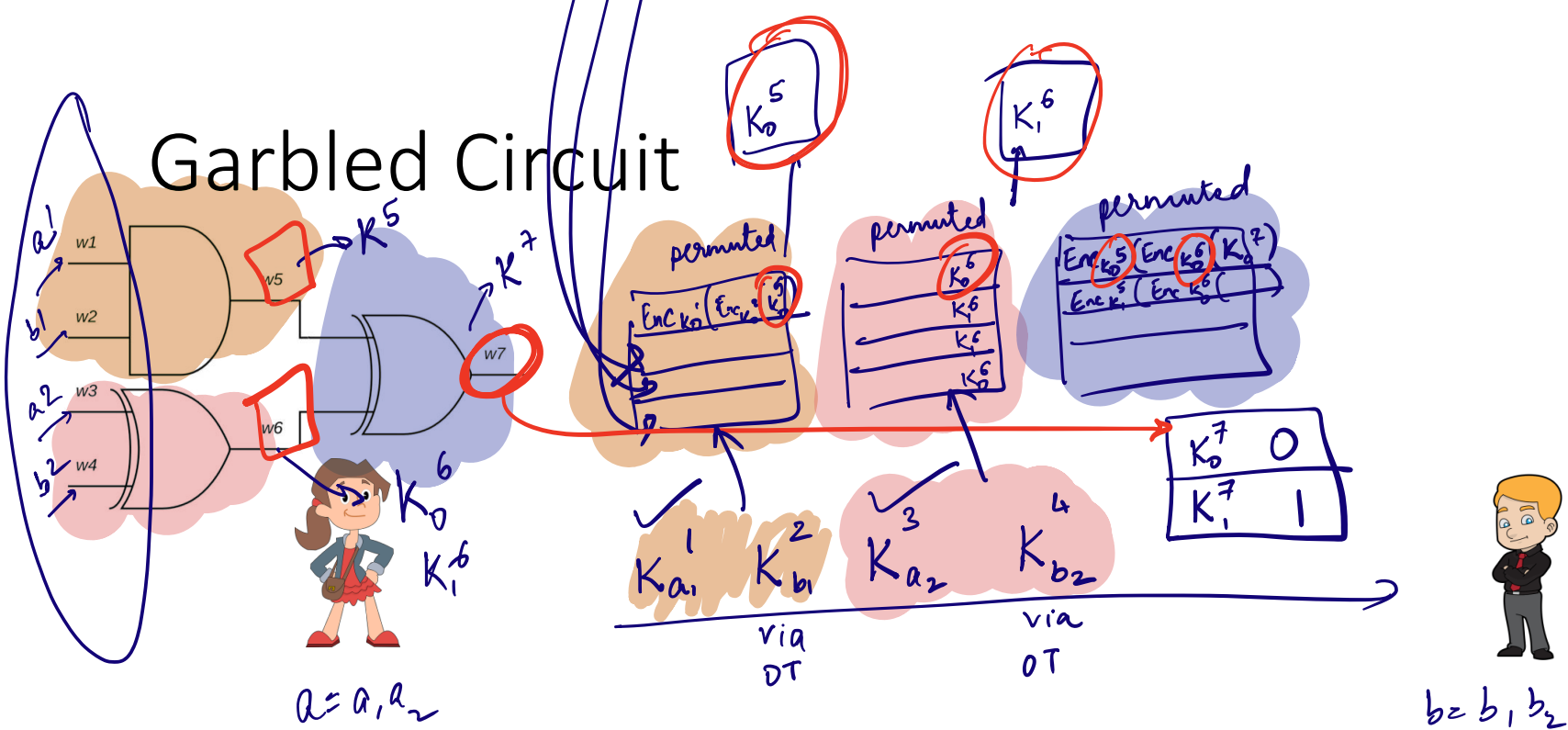
out of (K_0^2, K_1^2) Alice wants to send K_b^2 to Bob where b is Bob's choice bit

$C(a, b)$

K_a^1, K_b^2

K_0^5	0
K_1^5	1

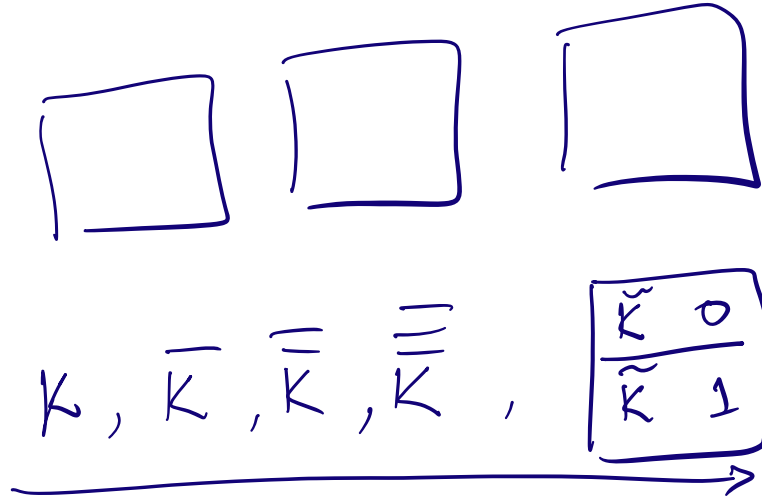
Garbled Circuit



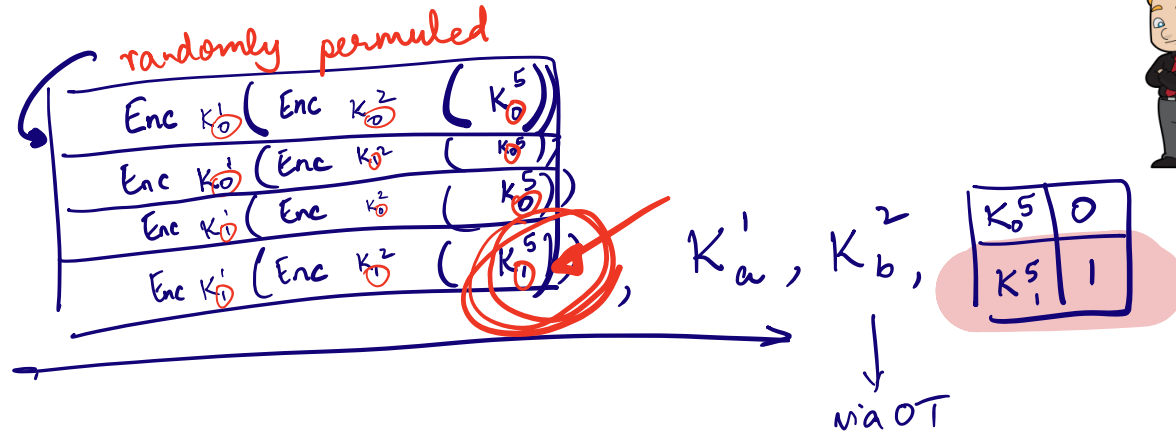
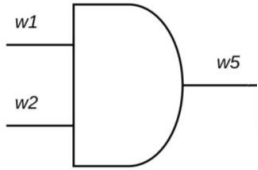
CORRECTNESS.

$C(a, b)$

Garbled Circuit: Security



Garbled Gate: Security



Garbled Gate: Security

H.W. : reduce to CPA security

Sample K_5^0, K_5^1 at random



$$C(a,b) = 1$$

send these keys

Simulated
Garbled Table

$\text{Enc}_K(\text{Enc}_{\bar{K}}(0))$
$\text{Enc}_K(\text{Enc}_{\bar{K}}(K_5^1))$
$\text{Enc}_{\hat{K}}(\text{Enc}_{\bar{K}}(0))$
$\text{Enc}_{\hat{K}}(\text{Enc}_{\bar{K}}(0))$

o/p map

K_5^0	0
K_5^1	1



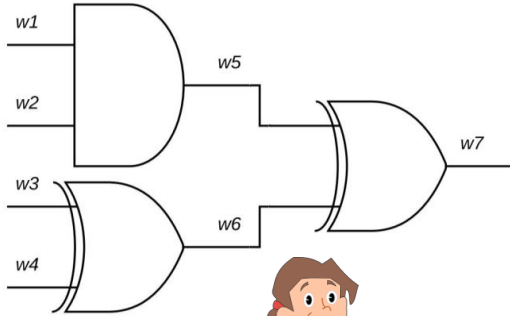
, K, \bar{K}



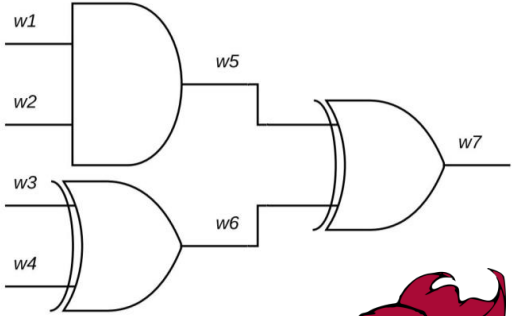
Garbled Gate: Security



Garbled Circuit: Security



Garbled Circuit: Security



Garbled Circuit: Security

