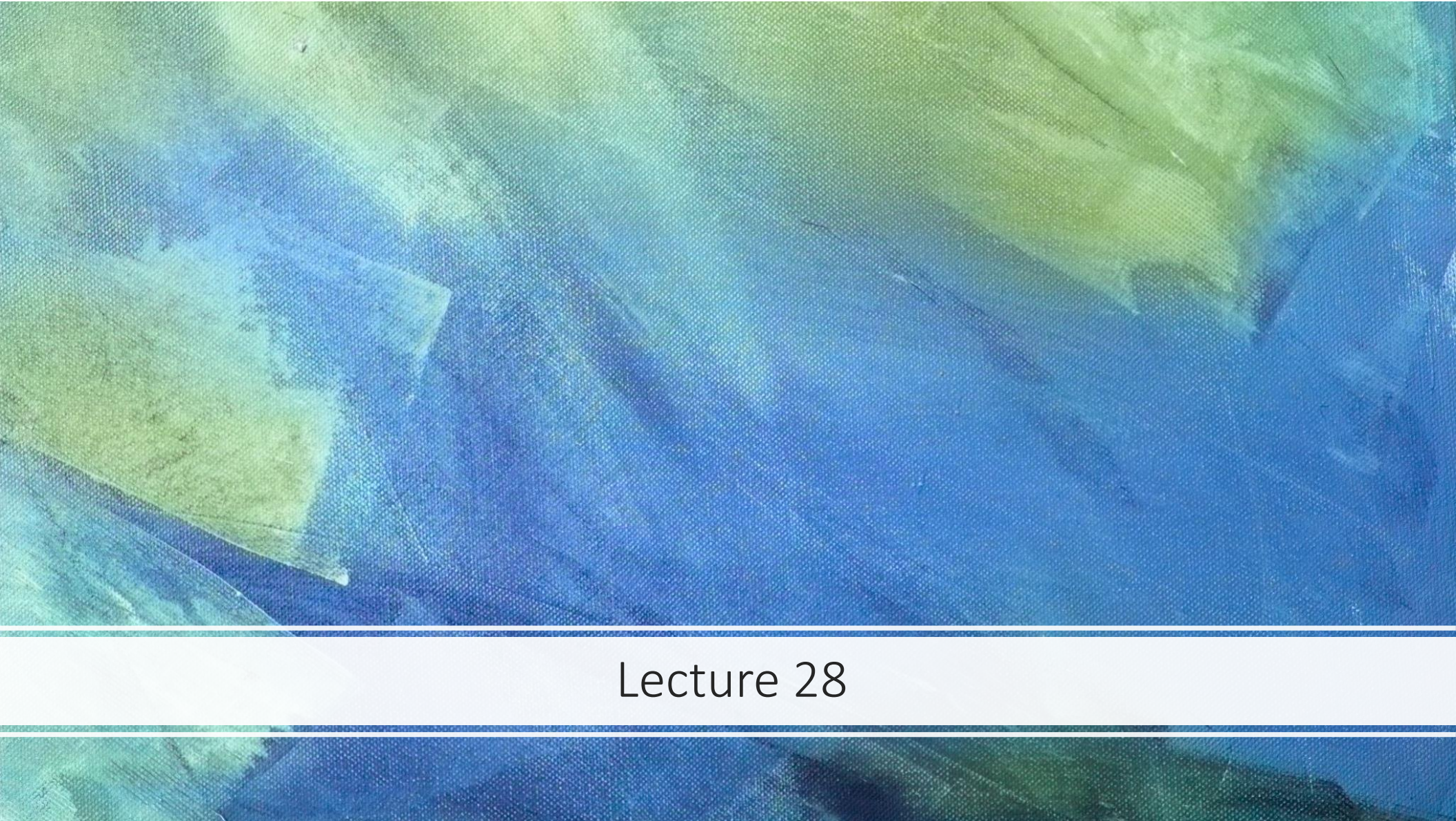
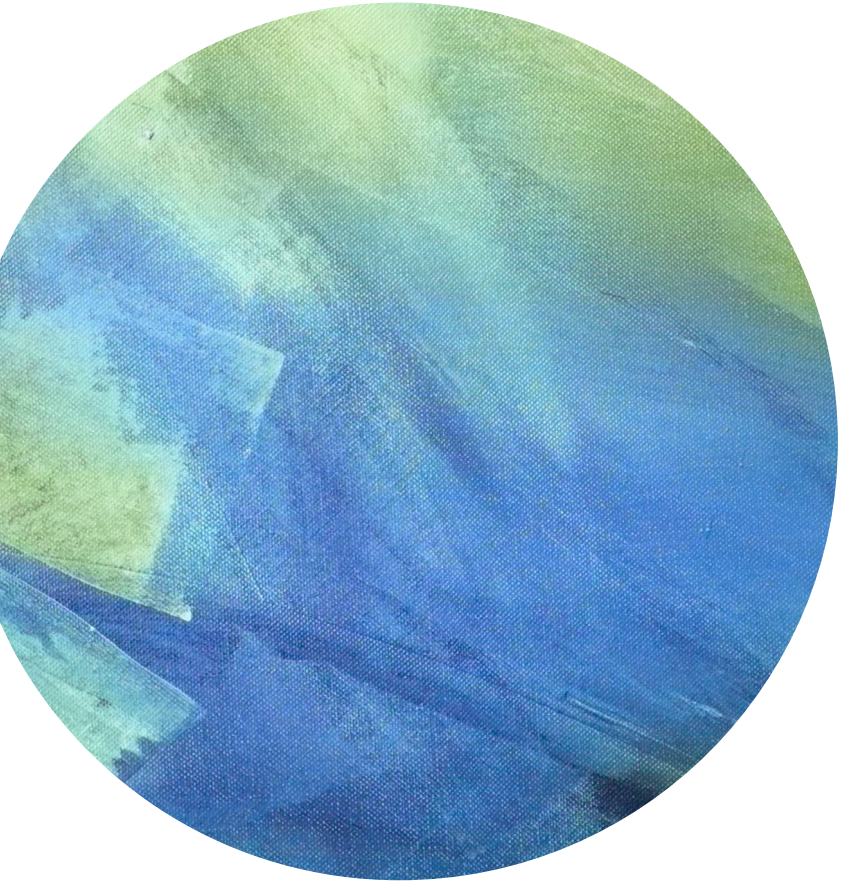


Lecture 28

Scribe : Fangqi

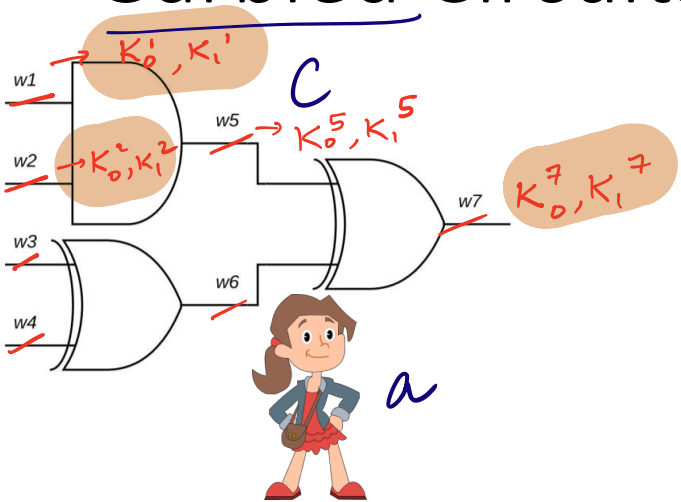


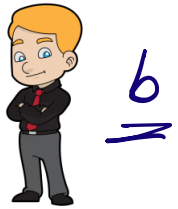
Outline

Garbled Circuits

Security

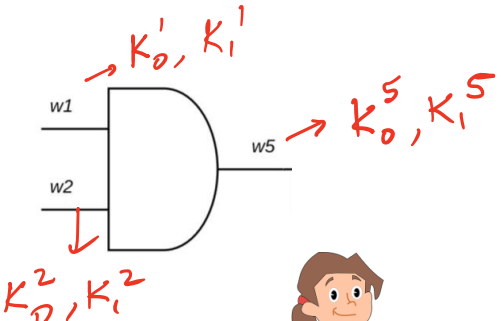
Garbled Circuits





$C(a, b)$

Garbled Gate



Garbled Table

w1	w2	w5
0	0	0
0	1	0
1	0	0
1	1	1

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

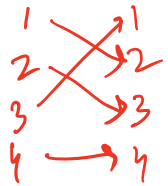
randomly permuted

Enc K_0^1 (Enc K_0^2 (K_0^5))
Enc K_0^1 (Enc K_1^2 (K_0^5))
Enc K_1^1 (Enc K_0^2 (K_0^5))
Enc K_1^1 (Enc K_1^2 (K_1^5))

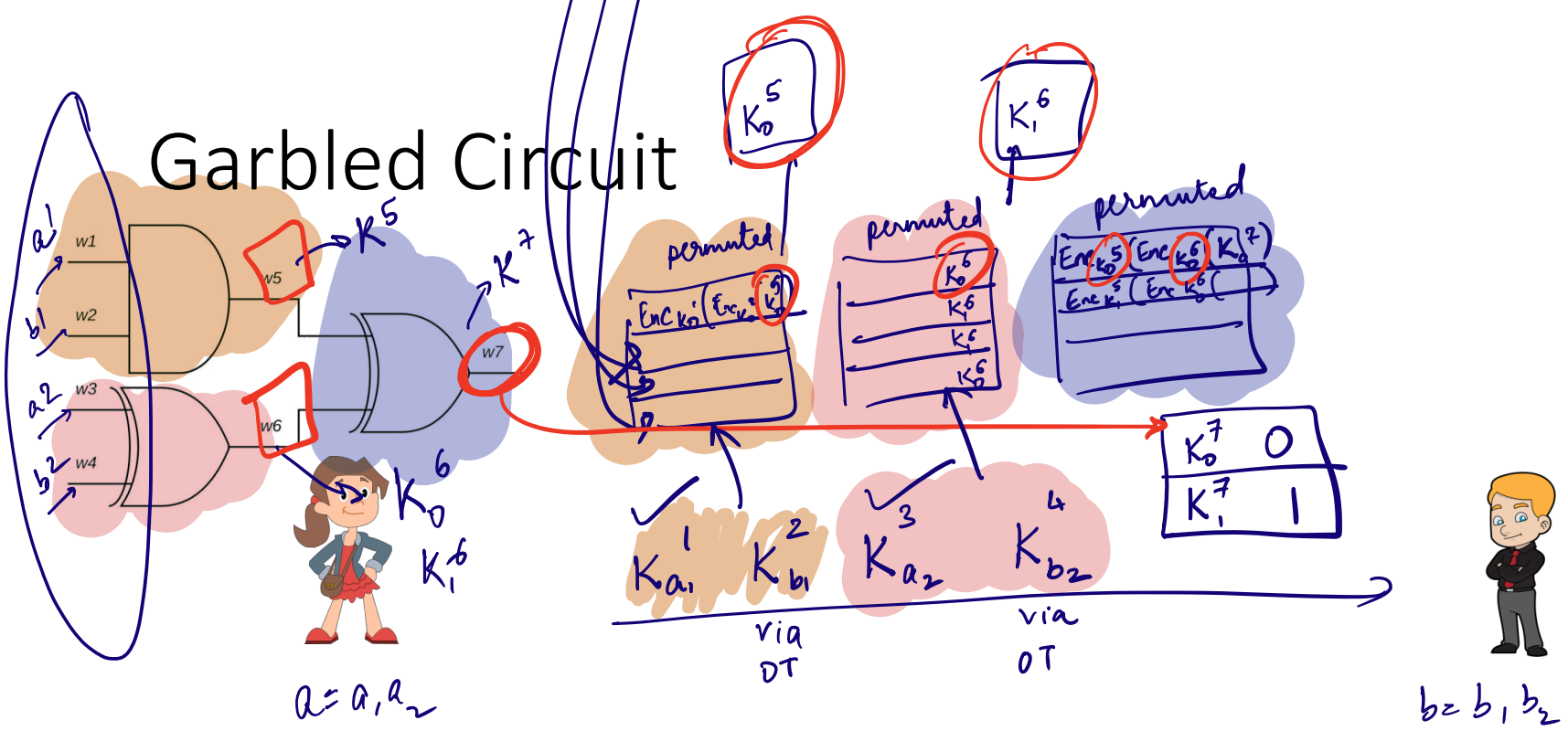
C(a, b)

$K_a^1, K_b^2,$

K_0^5	0
K_1^5	1



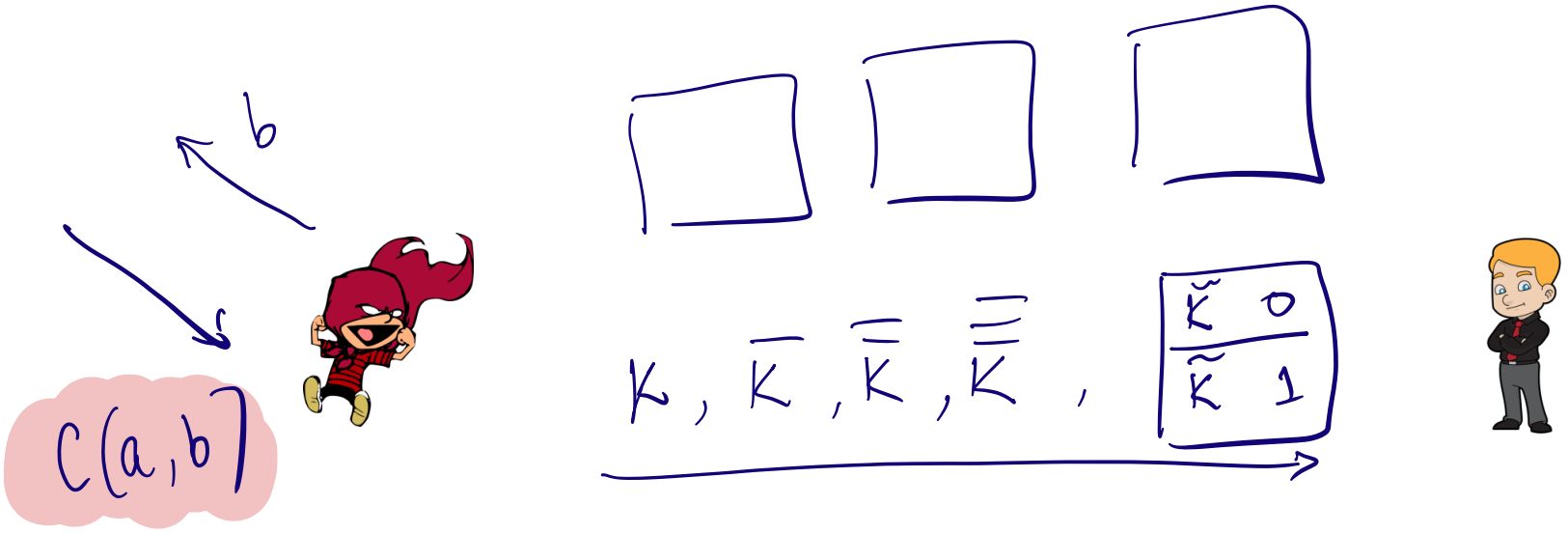
Garbled Circuit



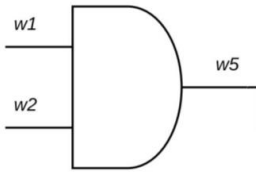
CORRECTNESS.

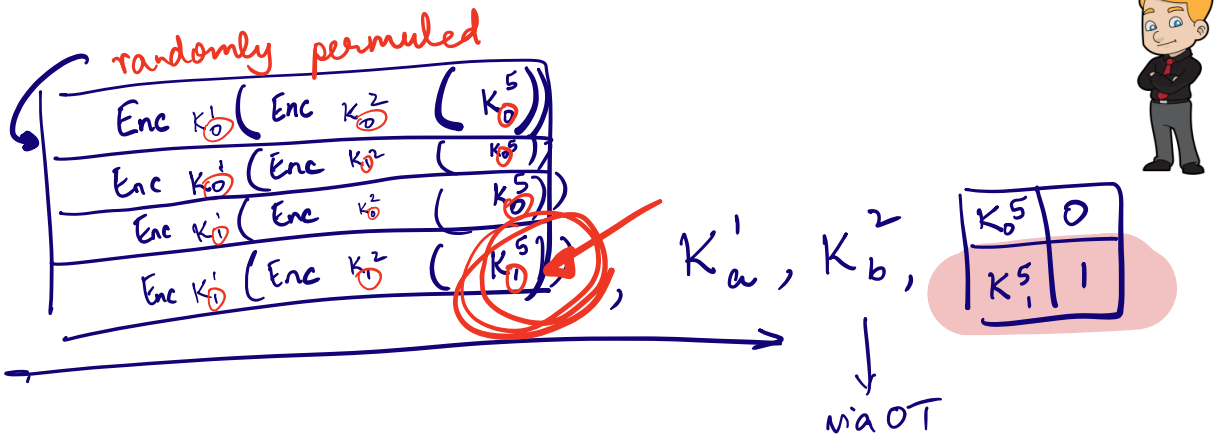
C(a, b)

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

$Enc_K(Enc_{\bar{K}}(0))$
$Enc_K(Enc_{\bar{K}}(K_5^1))$
$Enc_{\hat{K}}(Enc_{\bar{\hat{K}}}(0))$
$Enc_{\hat{K}}(Enc_{\bar{\hat{K}}}(0))$

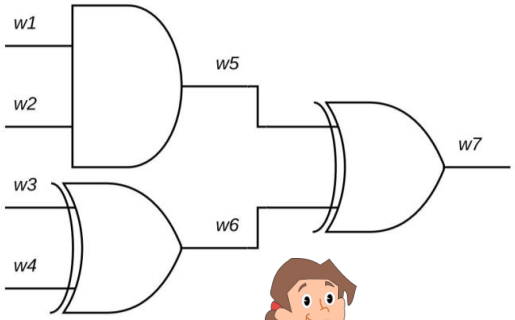
o/p map

K_5^0	0
K_5^1	1

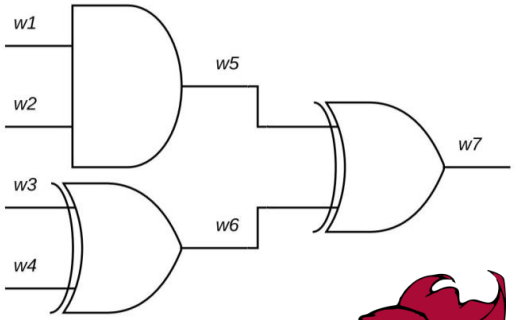
, $K, \bar{K}$

Garbled Gate: Security

Garbled Circuit: Security



Garbled Circuit: Security



Garbled Circuit: Security