

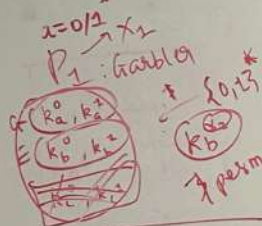
[Yao 82]

Garbled Circuit.
(semi-honest)

P_1, P_2

f single gate.

Enc
OT



k_a^0
 k_a^1

k_b^0 P_2

m, k $f: \{0,1\}^m \rightarrow \{0,1\}^n$

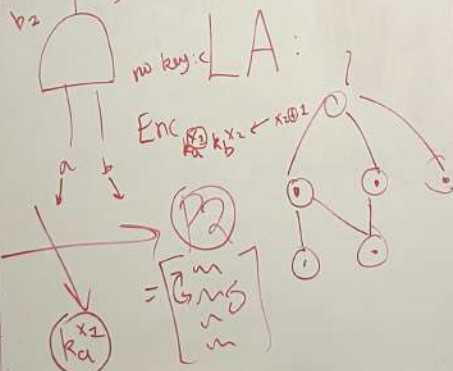
Evaluator

TA: $2^m \cdot 2^n$
exp bad!

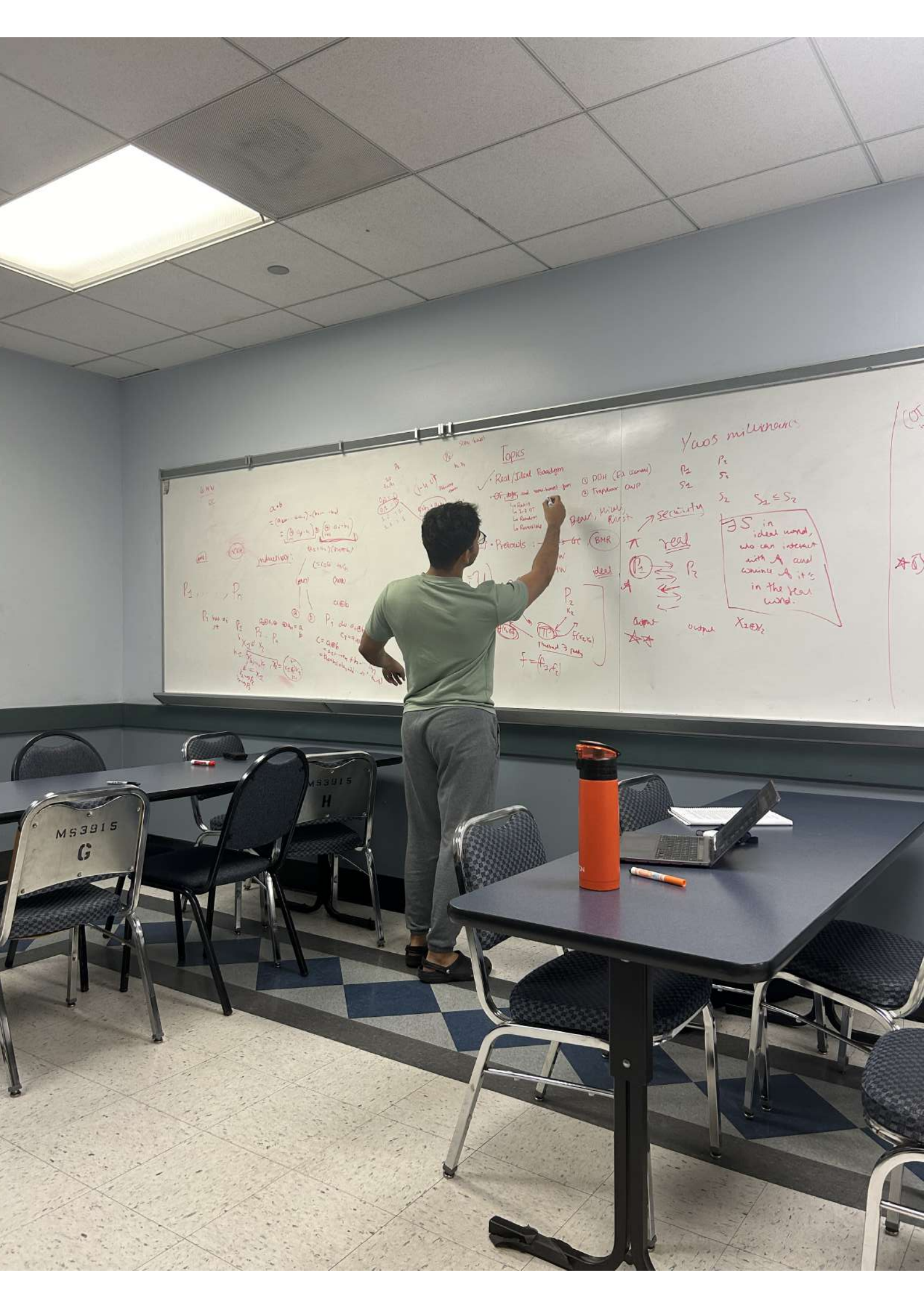
no key: LA

Enc $k_a^0, k_a^1 \leftarrow x_1 \oplus 1$

0,0	Enc $k_a^0, k_b^0(k_c^0)$	0
0,1	Enc $k_a^0, k_b^1(k_c^0)$	0
1,0	Enc $k_a^1, k_b^0(k_c^0)$	0
1,1	Enc $k_a^1, k_b^1(k_c^1)$	1



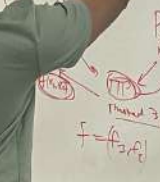
k_c^0 has k_a^0, k_b^0
Share out x_2
OT!
BUT! Share out k_c^1
Share out k_c^0
BUT! You're for n players.



Topics

- Real/Ideal Realization
- Eff. diff. and semi-honest form
- Le GSW
- Le 2-3 OT
- Le Random
- Le Random

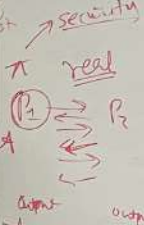
• Products: \rightarrow or \leftarrow (BMR)



Yao's millennium

P_1 S_1
 P_2 S_2
 $S_2 \in S_2$

in ideal world, who can interact with A and convince A it's in the real world.



G. H. W
OT

$$a \cdot b = (a_1 a_2 \dots a_n) \cdot (b_1 b_2 \dots b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$$

$$= (\bigoplus_{i=1}^n a_i \cdot b_i) \oplus (\bigoplus_{i=1}^n a_i \cdot b_i)$$

AND

XOR

inductively:

P_1, \dots, P_n

P_i has a_i

$P_1 \dots P_n$
 $x_1 \dots x_n$

$$n \rightarrow \sum_{i=1}^n x_i, \quad x_i = (x_{i1} \oplus x_{i2} \oplus \dots \oplus x_{in})$$

$$a_2 + a_1 \cdot (b_2 + b_1)$$

$$= (a_2 \oplus a_1) \cdot (b_2 \oplus b_1)$$

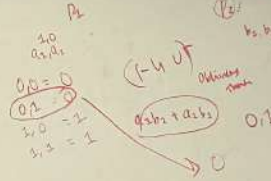
$$(AND) \quad (XOR)$$

$$a \oplus b$$

$$C = a \oplus b$$

$$= a_1 \oplus a_2 \oplus \dots \oplus a_n + b_1 \oplus b_2 \oplus \dots \oplus b_n$$

$$= (a_1 + b_1) \oplus (a_2 + b_2) \oplus \dots \oplus (a_n + b_n)$$



semi-honest

Topics

Real/Ideal Paradigm

- OT, sign, and semi-honest gen
- Robust
- 2-2 OT
- Random
- Reversible

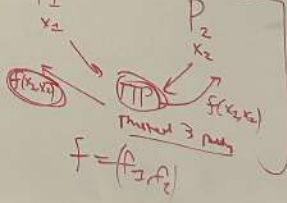
- DDH (ElGamal)
- Tripdoor OWP

Beau, Nicks, Rivest

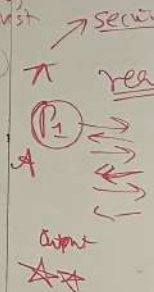
$\{0, 1\}^n$ Protocols

- Yao's
- BGW
- GMW

P_1, P_2



ideal





Topics:

Real/Ideal Paradigm

OT, diff, and commitment from

- Robinson
- 2-2 OT
- Random
- Reversible

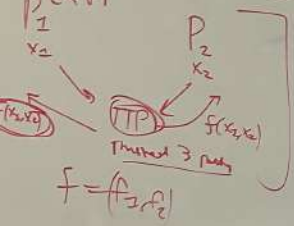
- DDH (ElGamal)
- Trapdoor OWP

Beal, Nicali, Rivest

Protocols: - Yao's GC, (BMR)

- BGW

- GMW



Yao's millennium

P_1 P_2
 S_1 S_2
 $S_2 \leq S_1$

Security

π real

ideal

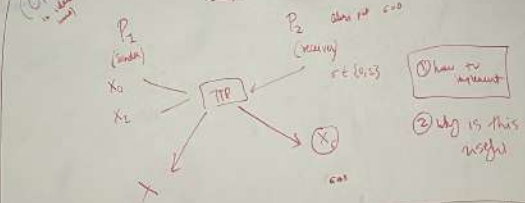
P_1 P_2

output

$x_1 \otimes x_2$

$\exists S$ in ideal world, who can interact with A and convince it it's in the real world.

OT (semi-honest)



Why OT impossible info-theoretic

DDH

for

OT is completable for PR.
 Decisional Diff. Assumption:
 $x, y \in \mathbb{Z}_p$
 $(g, g^x, g^y, g^{xy}) \approx (g, g^x, g^y, g^{z^2})$

OWP:
 $f: \{0,1\}^n \rightarrow \{0,1\}^n$
 s.t. $f(x) \neq f(y)$
 not given $x, y \in \{0,1\}^n$
 different $f(x, y)$

