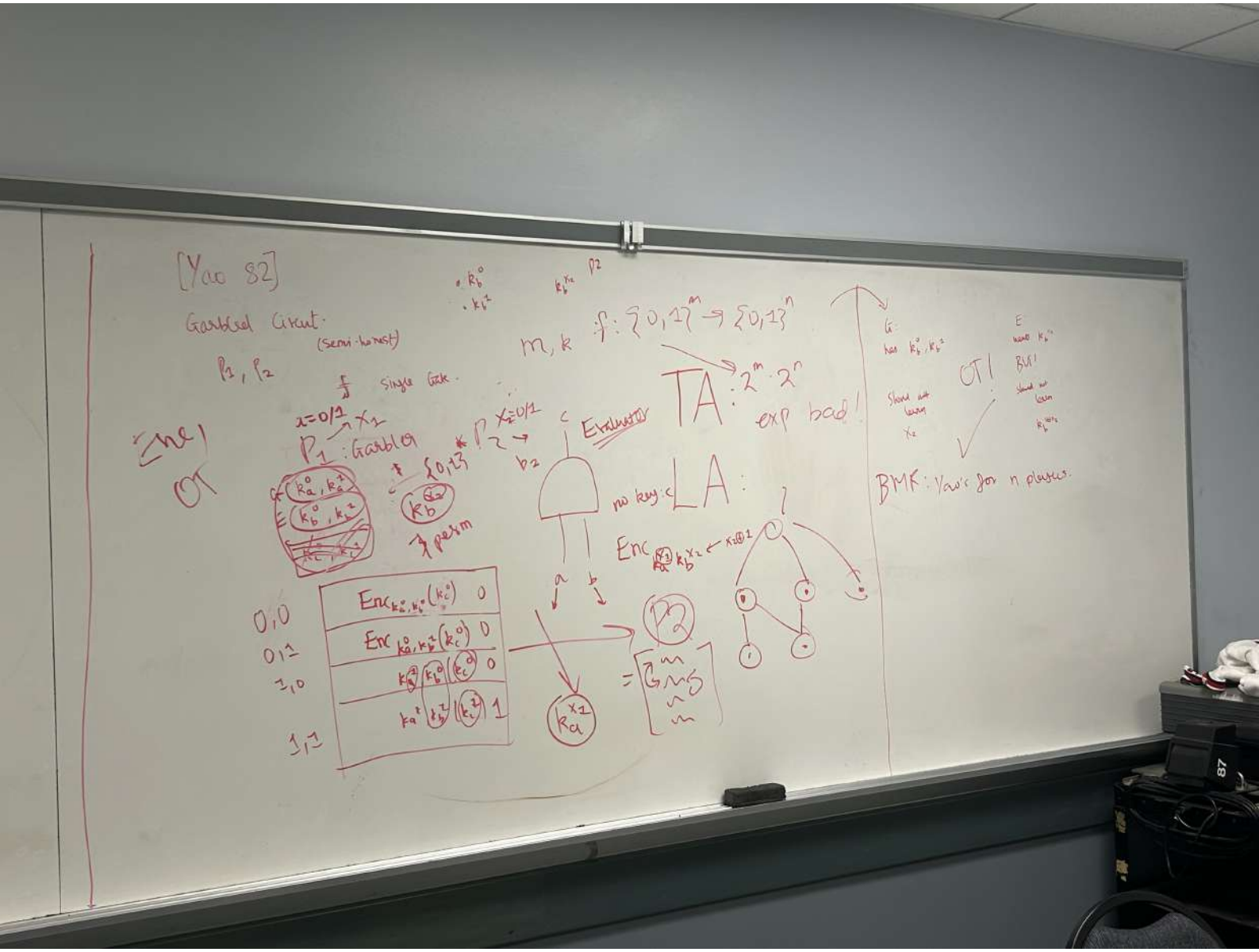
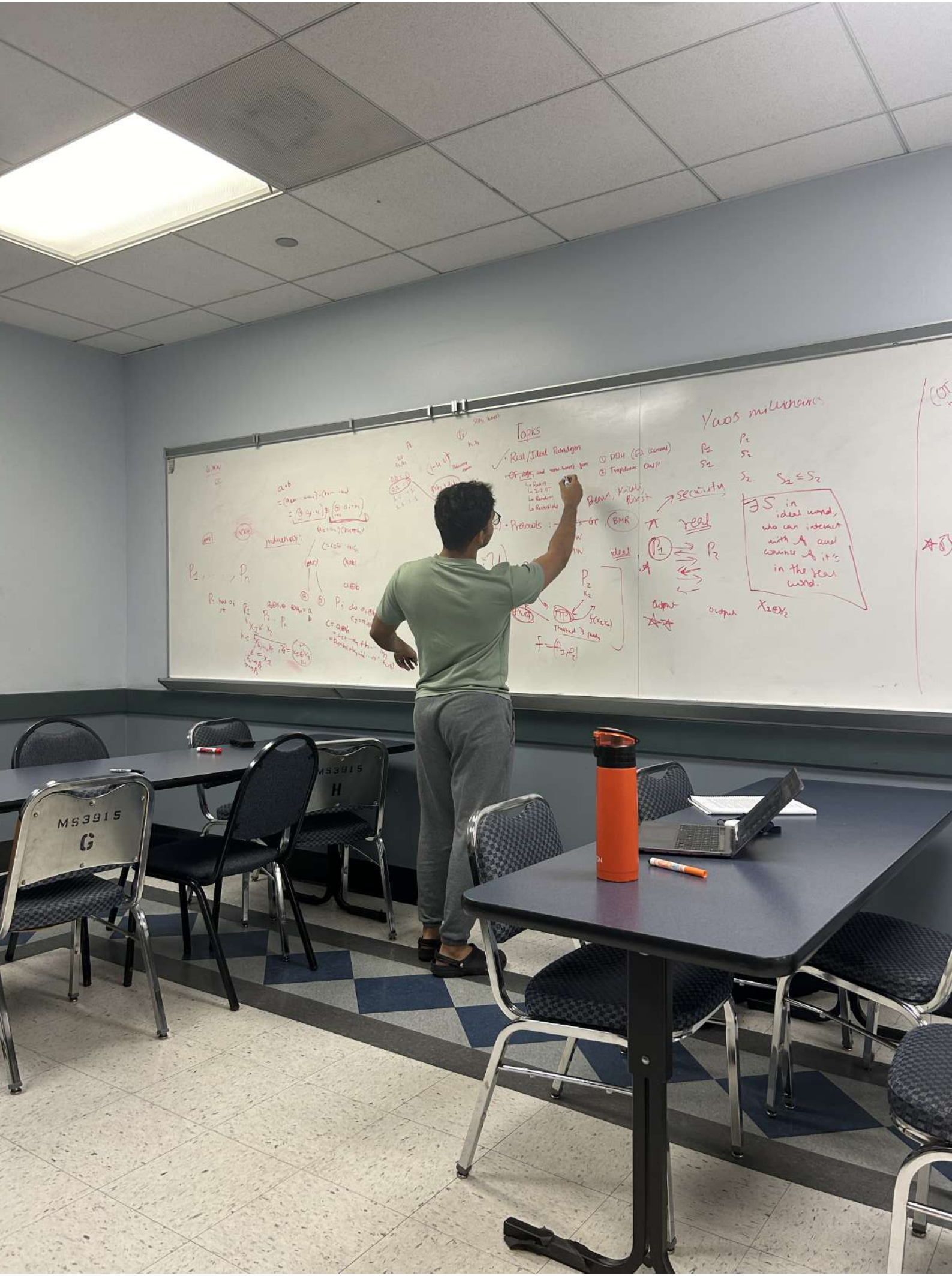
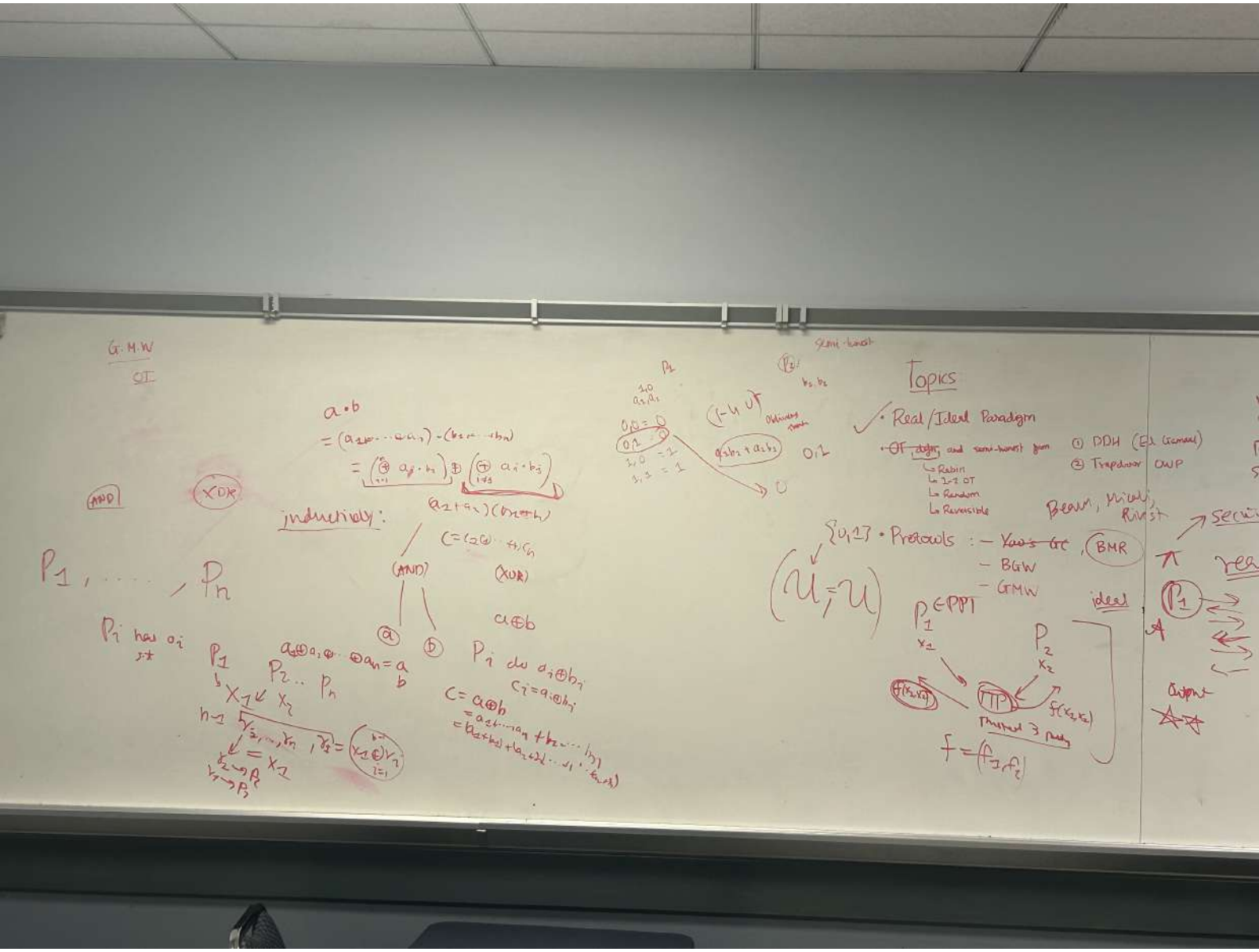
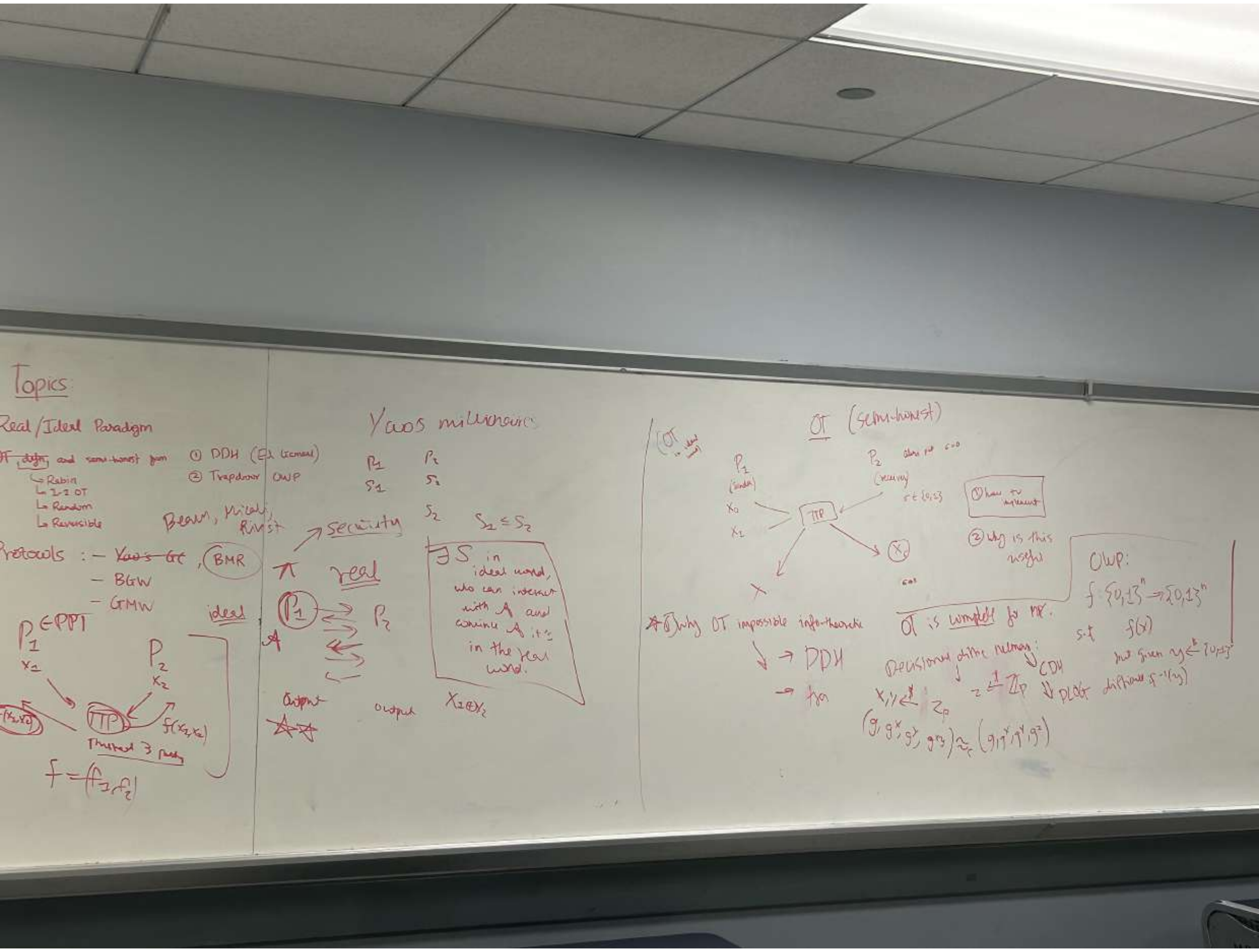

[Yao 82]
Garbled Circuit
(semi-honest)
P1, P2
Single Gate
TA
exp bad!
LA
OT
BMK: Yao's for n players.

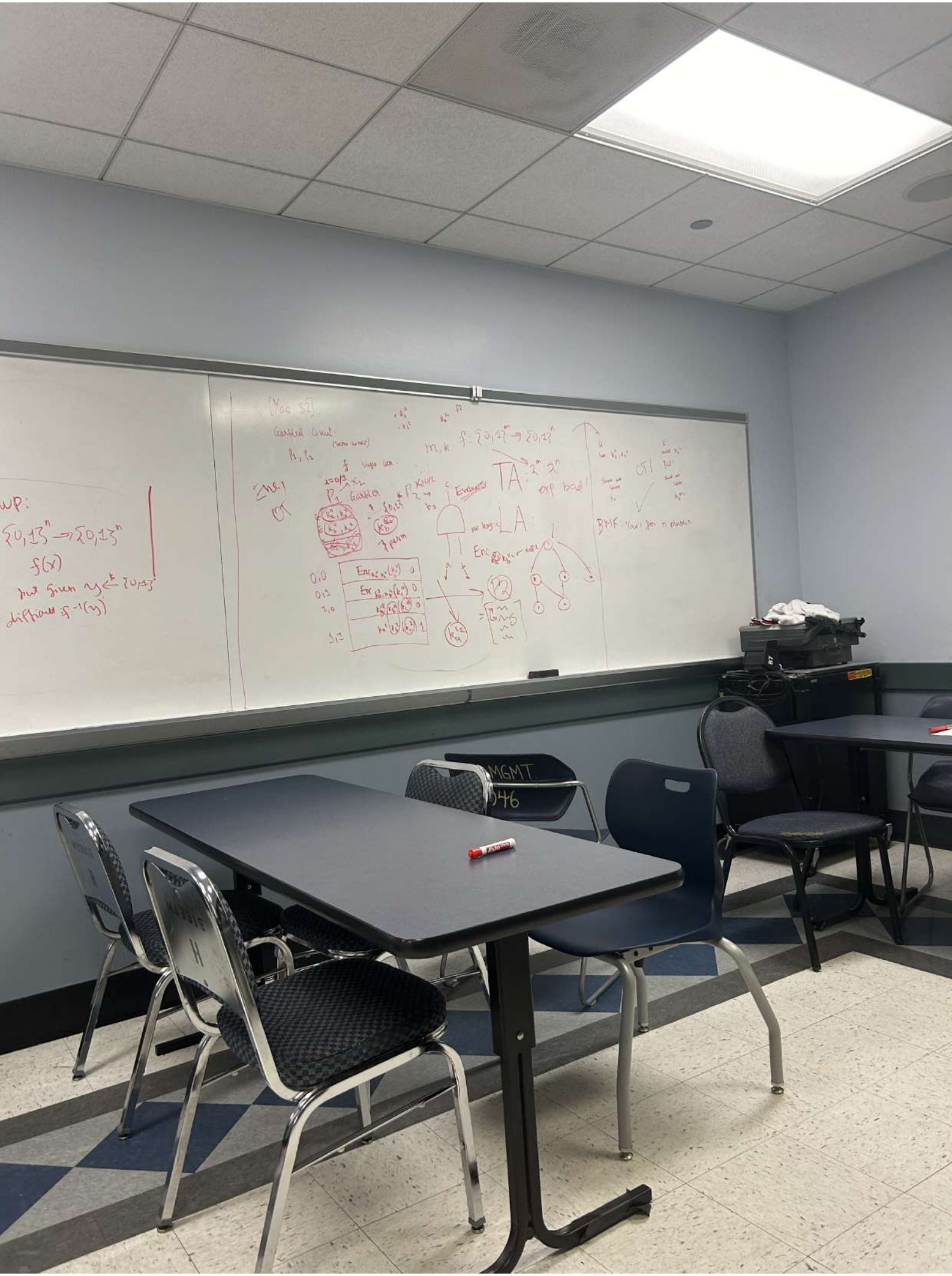

Topics
Yaos millionaire
Real/Ideal Paradigm
Protocols
BMR
GMW
security
real
ideal
MS3915
G
MS3915
H


G.M.W
OT
Topics
Real/Ideal Paradigm
DDH (EL Gamal)
Trapdoor OWP
Rabin
1-2 OT
Random
Reversible
Protocols
BMR
BGW
GMW
ideal
TTP
AND
XOR
$P_1, \ldots, P_n$
P_i has o_i
induction


Please do not add or remove furniture from the classroom.



Topics:
Real/Ideal Paradigm
① DDH (El Gamal)
② Trapdoor OWP
Rabin
1-2 OT
Random
Reversible
Protocols
BGW
GMW
BMR
Beaver, Micali, Rivest
Yao's millionaires
P1
P2
S1
S2
S2 ≤ S2
security
real
ideal
P1 ∈ PPT
P2
x1
x2
TTP
f(x1,x2)
Trusted 3 party
f = (f1, f2)
∃ S in ideal world, who can interact with A and convince A it's in the real world.
Output
output
x1⊕x2
OT (semi-honest)
P1
(sender)
P2
(receiver)
x0
x1
TTP
① how to implement
② why is this useful
OT is complete for MPC.
why OT impossible info-theoretic
→ DDH
OWP:
f: {0,1}^n → {0,1}^n
s.t. f(x)
Decisional diffie hellman
CDH
DLOG
(g, g^x, g^y, g^xy) ≈c (g, g^x, g^y, g^z)


MGMT
046