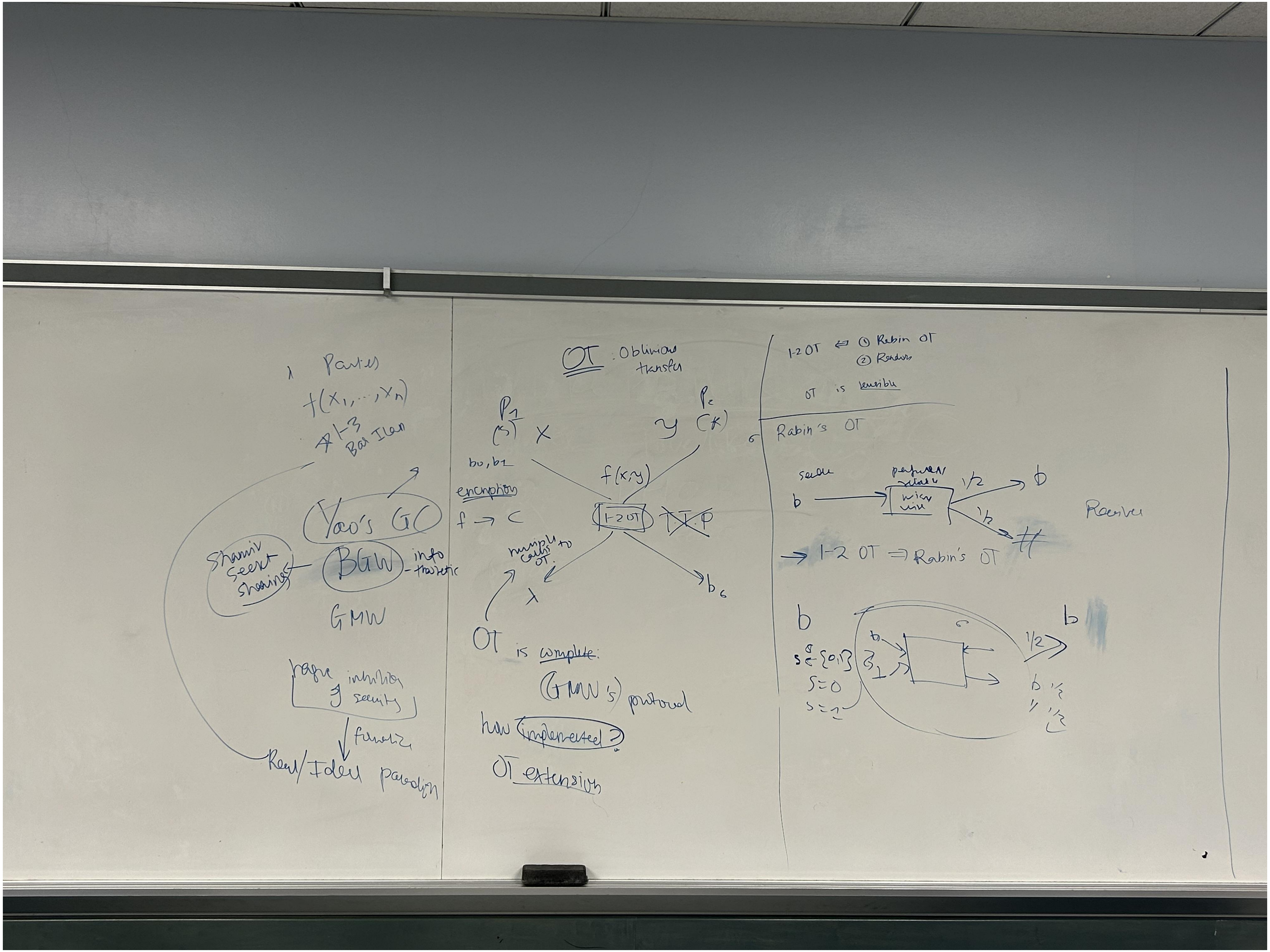
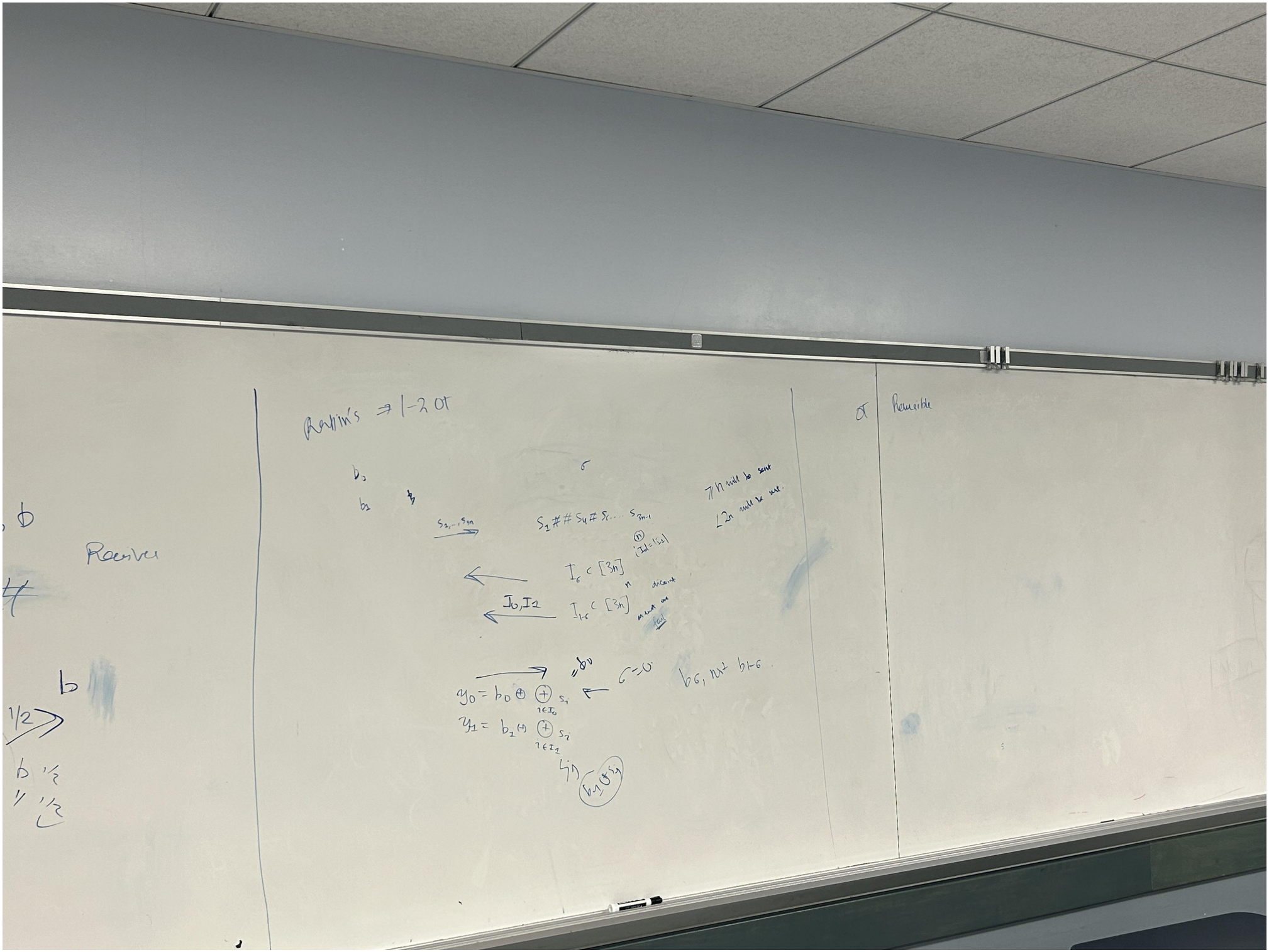
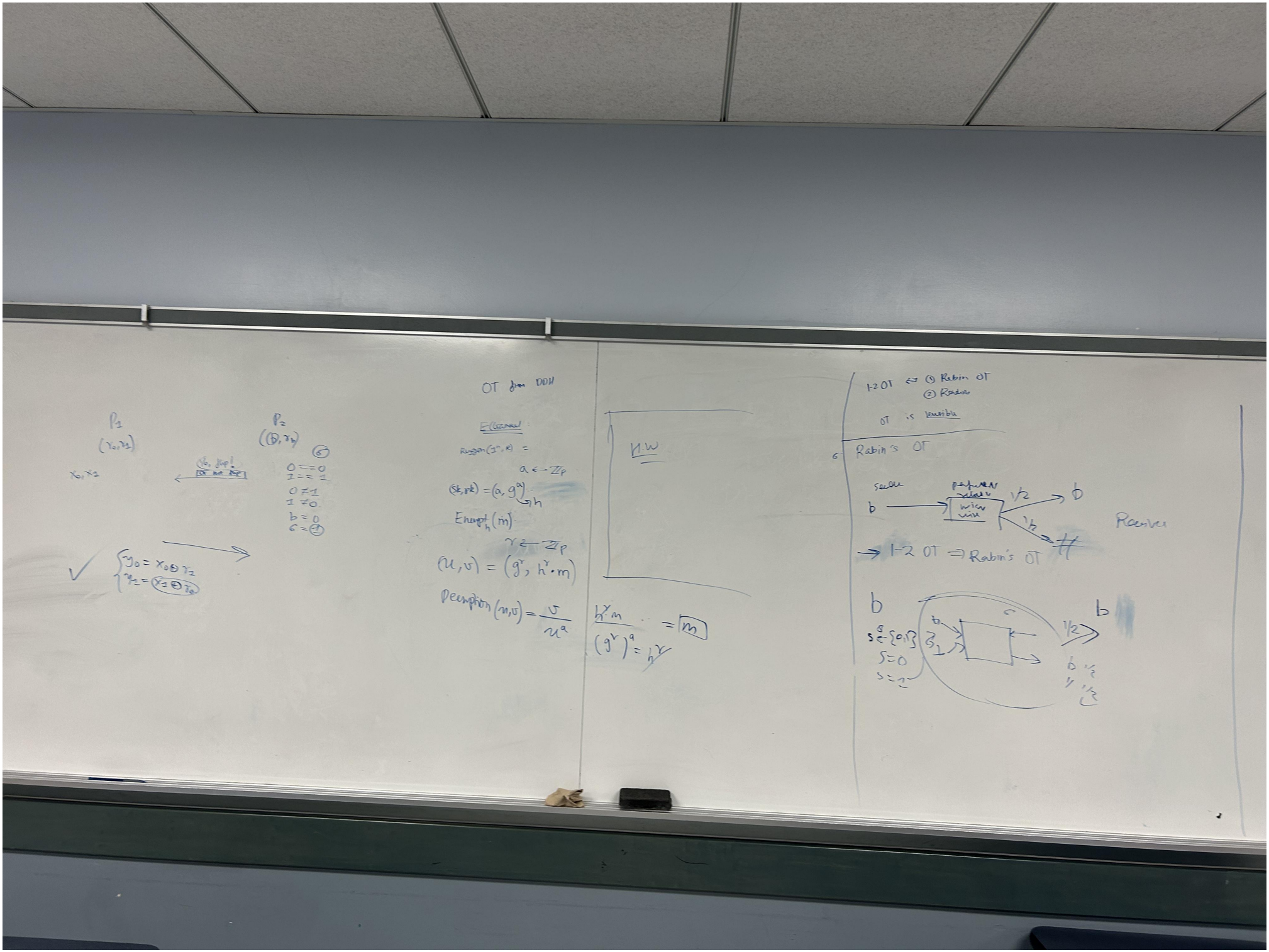
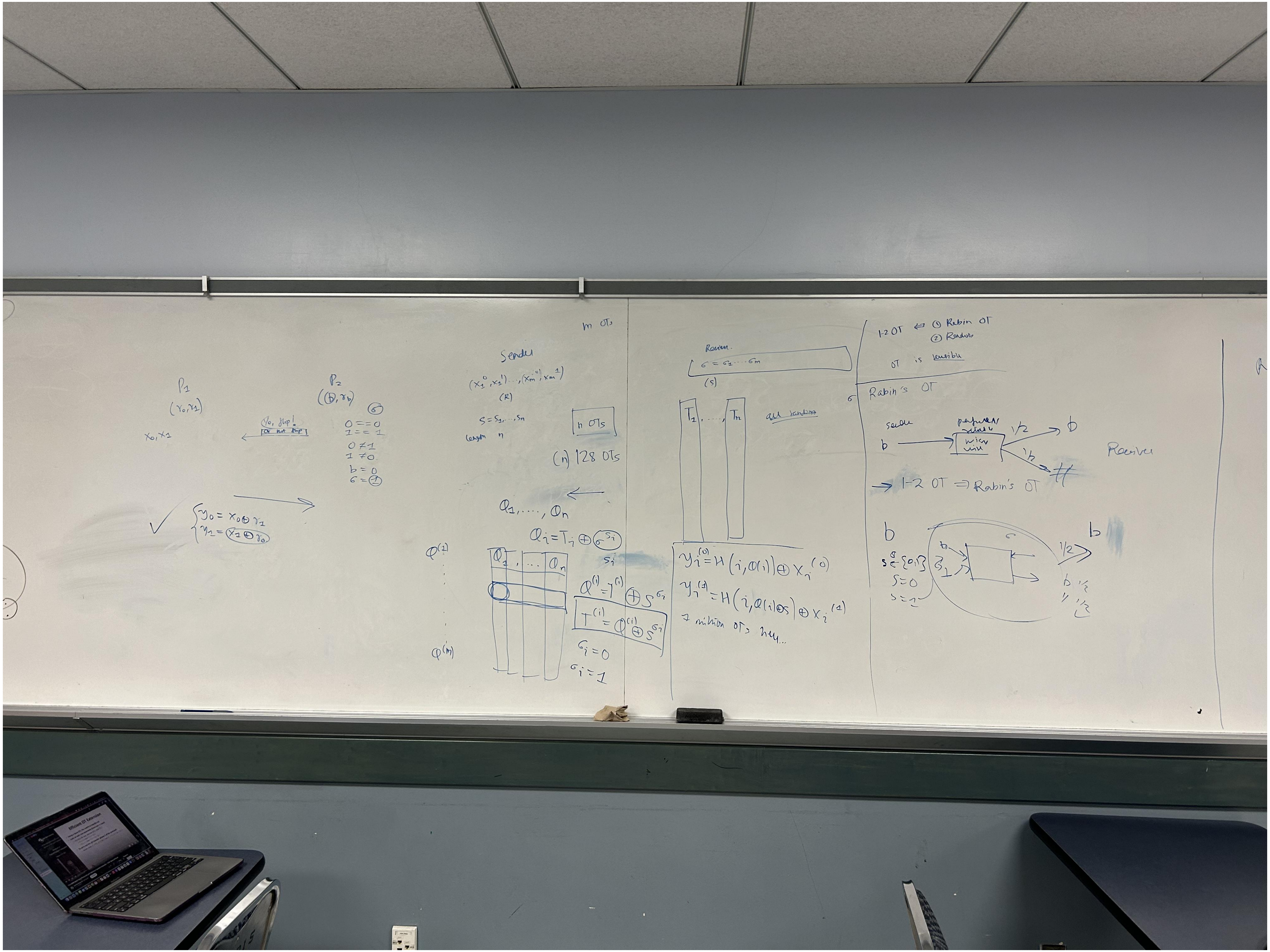


Parties
f(x1, ..., xn)
Bar Ilan
Yao's GC
Shamir secret sharing
BGW
info theoretic
GMW
vague intuition of security
formalize
Real/Ideal paradigm
OT : Oblivious transfer
P1
P2
x
y
b0, b1
encryption
f → C
f(x,y)
1-2 OT
T.T.P
multiple calls to OT
b_σ
OT is complete:
(GMW's) protocol
how implemented?
OT extension
1-2 OT ⇐ ① Rabin OT
② Random
OT is reversible
Rabin's OT
Sender
Receiver
b
1/2
#
1-2 OT ⇒ Rabin's OT
s ← {0,1}
s=0
s=1


Receiver
Remainder
$y_0 = b_0 \oplus \bigoplus_{i \in I_0} s_i$
$y_1 = b_1 \oplus \bigoplus_{i \in I_1} s_i$

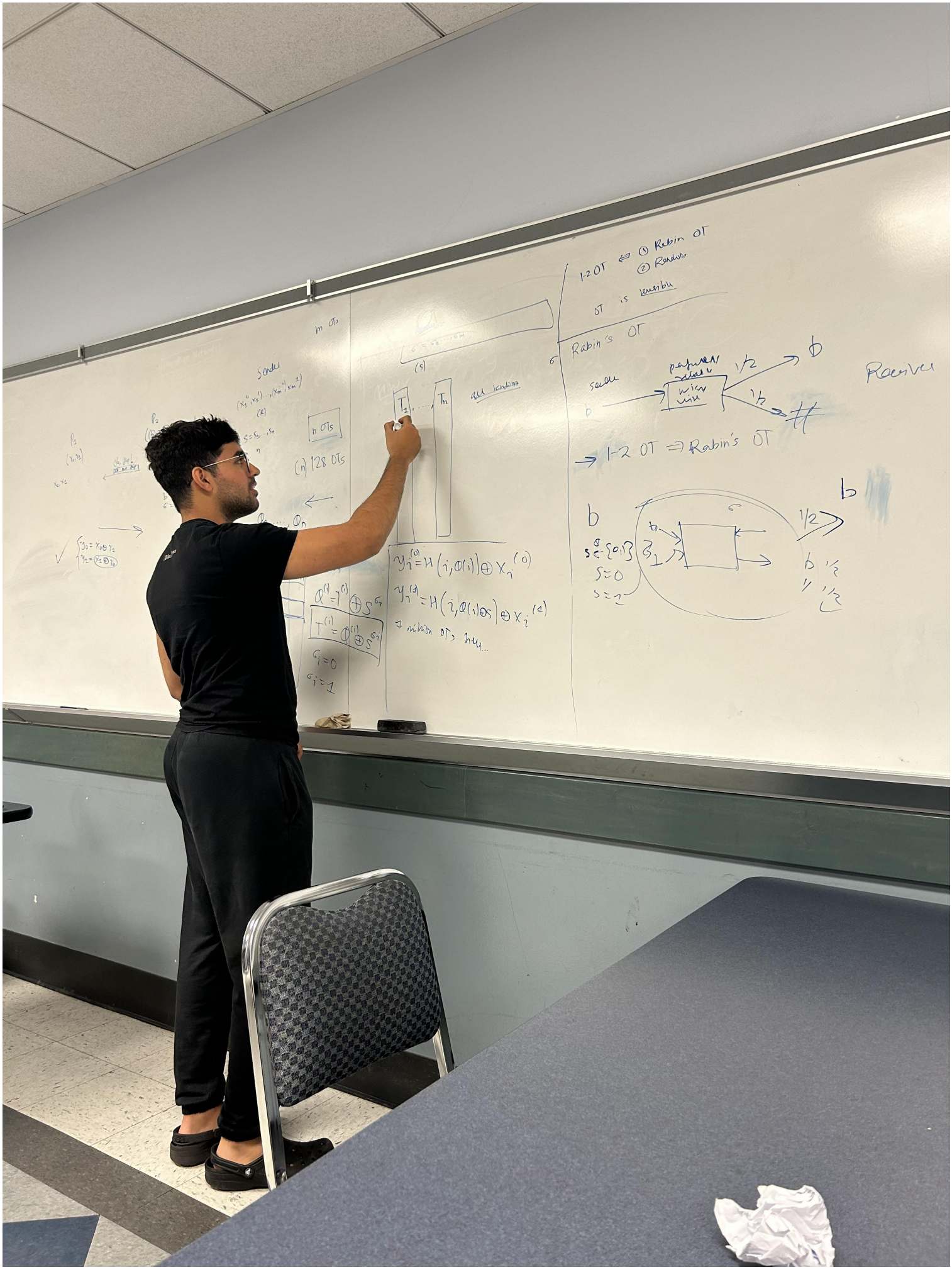

OT from DDH
1-2 OT ⇔ ① Rabin OT
② Reduction
OT is reversible
Rabin's OT
Receiver
1-2 OT ⇒ Rabin's OT


MS 3915
A



m OTs
Sender
P1
P2
n OTs
(n) 128 OTs
Q1, ..., Qn
Receiver
T1, ..., Tn
1 million OTs hey...
1-2 OT ⇔ (1) Rabin OT
(2) Random
OT is reversible
Rabin's OT
Sender
Receiver
1-2 OT ⇒ Rabin's OT
Efficient OT Extension


1-2 OT ⇐ ① Rabin OT
② Random
OT is reversible
Rabin's OT
1-2 OT ⇒ Rabin's OT
Sender
1/2
pause and ponder.


1-2 OT ⇐ ① Rabin OT
② Rabin
OT is invertible
Rabin's OT
1/2
1/2
Receiver
→ 1-2 OT ⇒ Rabin's OT
(n) 128 OTs