

Rewlin's \Rightarrow 1-2 OT

Receiver

b_1

b_2

$s_{3n-1} s_m$

s'

$s_1 \# s_4 \# s_5 \dots s_{3n-1}$

①

$(I_0 = I_1)$

7 bits to sent

12 bits to use

$I_0 \subset [3n]$

\leftarrow

I_0, I_1

$I_1 \subset [3n]$

\leftarrow

I_1

distinct

and

well

$$y_0 = b_0 \oplus \bigoplus_{i \in I_0} s_i$$

$$y_1 = b_1 \oplus \bigoplus_{i \in I_1} s_i$$

y_1

$\bigoplus_{i \in I_1} s_i$

$$\Rightarrow C=0$$

$b_0, n \neq b_1, 6$

OT
Reversible

$$\begin{array}{ccc}
 P_1 & & P_2 \\
 (\gamma_0, \gamma_2) & & (\beta_0, \beta_2) \quad \textcircled{5} \\
 x_0, x_2 & \xleftarrow{\text{Bob, Alice!}} & \\
 \end{array}$$

$\begin{aligned} 0 &= 0 \\ 2 &= 1 \\ 0 &\neq 1 \\ 1 &\neq 0 \\ b &= 0 \\ \beta &= \textcircled{5} \end{aligned}$

$\checkmark \begin{cases} \gamma_0 = x_0 \oplus \gamma_2 \\ \gamma_2 = (x_2 \oplus \beta_0) \end{cases}$

ElGamal

Rusen (G^n, \mathbb{G}) =

$a \in \mathbb{Z}_P$

$(sk, pk) = (a, g^a)$

$h = g^a$

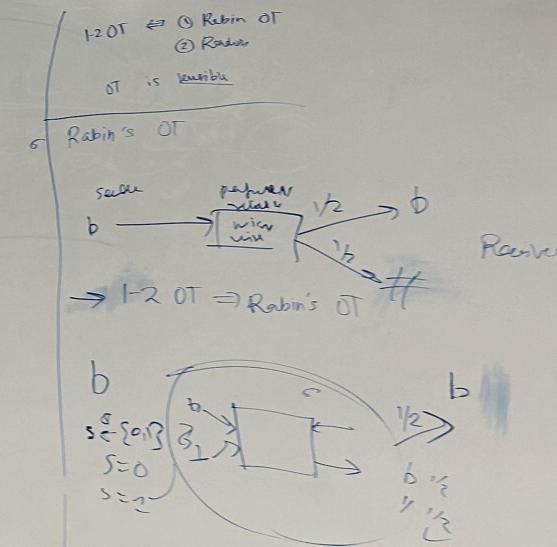
$E_{pk}(m)$

$\gamma \in \mathbb{Z}_P$

$(U, V) = (g^\gamma, h^\gamma \cdot m)$

Decryption (m, V) = $\frac{V}{U^\alpha} = m$

$$\begin{array}{c}
 \boxed{U, V} \\
 \downarrow \\
 \frac{h^\gamma m}{(g^\gamma)^\alpha} = m
 \end{array}$$



ANM's \Rightarrow 1-2 OT

Receiver

b_2

b_1

$s_{21} s_{12}$

s_1

s_2

s_3

s_4

s_5

s_6

s_7

s_8

$$T_e \in [2^8]$$

$$T_e \in [2^8]$$

$$y_0 = b_0 e + s_0$$

$$y_1 = b_1 e + s_1$$

$$y_2 = b_2 e + s_2$$

$$y_3 = b_3 e + s_3$$

$$y_4 = b_4 e + s_4$$

$$y_5 = b_5 e + s_5$$

$$y_6 = b_6 e + s_6$$

$$y_7 = b_7 e + s_7$$

$$y_8 = b_8 e + s_8$$

$$y_9 = b_9 e + s_9$$

$$y_{10} = b_{10} e + s_{10}$$

$$y_{11} = b_{11} e + s_{11}$$

$$y_{12} = b_{12} e + s_{12}$$

Δ Error

\Rightarrow 0.6

0.5

0.4

0.3

0.2

0.1

0.0

-0.1

-0.2

-0.3

-0.4

-0.5

-0.6

-0.7

-0.8

-0.9

-1.0

p_{11}

p_{12}

p_{13}

p_{14}

p_{15}

p_{16}

p_{17}

p_{18}

p_{19}

p_{10}

p_{11}

p_{12}

p_{13}

p_{14}

p_{15}

p_{16}

p_{17}

p_{21}

p_{22}

p_{23}

p_{24}

p_{25}

p_{26}

p_{27}

p_{28}

p_{29}

p_{20}

p_{21}

p_{22}

p_{23}

p_{24}

p_{25}

p_{26}

p_{27}

p_{31}

p_{32}

p_{33}

p_{34}

p_{35}

p_{36}

p_{37}

p_{38}

p_{39}

p_{30}

p_{31}

p_{32}

p_{33}

p_{34}

p_{35}

p_{36}

p_{37}

p_{41}

p_{42}

p_{43}

p_{44}

p_{45}

p_{46}

p_{47}

p_{48}

p_{49}

p_{40}

p_{41}

p_{42}

p_{43}

p_{44}

p_{45}

p_{46}

p_{47}

p_{51}

p_{52}

p_{53}

p_{54}

p_{55}

p_{56}

p_{57}

p_{58}

p_{59}

p_{50}

p_{51}

p_{52}

p_{53}

p_{54}

p_{55}

p_{56}

p_{57}

p_{61}

p_{62}

p_{63}

p_{64}

p_{65}

p_{66}

p_{67}

p_{68}

p_{69}

p_{60}

p_{61}

p_{62}

p_{63}

p_{64}

p_{65}

p_{66}

p_{67}

p_{71}

p_{72}

p_{73}

p_{74}

p_{75}

p_{76}

p_{77}

p_{78}

p_{79}

p_{70}

p_{71}

p_{72}

p_{73}

p_{74}

p_{75}

p_{76}

p_{77}





$$\begin{array}{ll}
 P_1 & P_2 \\
 (\gamma_0, \gamma_1) & ((\beta), \gamma_0) \quad \textcircled{6} \\
 \xrightarrow{x_0, x_1} & \xleftarrow{\substack{\gamma_0, \text{ flip!} \\ \text{or not flip?}}}
 \end{array}$$

$\begin{array}{l} 0 == 0 \\ 1 == 1 \\ 0 \neq 1 \\ 1 \neq 0 \\ b = 0 \\ s = \oplus \end{array}$

$$\checkmark \quad \begin{cases} y_0 = x_0 \oplus \gamma_1 \\ y_1 = x_1 \oplus \gamma_0 \end{cases}$$

Sender: $(x_0^0, x_1^0), \dots, (x_m^0, x_m^1)$
 (R)
 $S = S_{m+1, n}$ length n
 $m \text{ OTs}$
 $\text{(a) } 128 \text{ OTs}$

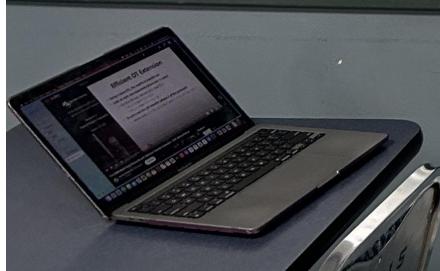
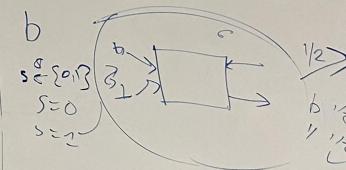
$\varphi^{(1)}, \dots, \varphi^{(n)}$
 $\varphi^{(1)}: \begin{array}{|c|c|} \hline 0_1, \dots, 0_n & \oplus \\ \hline \end{array} \quad \varphi^{(n)}: \begin{array}{|c|c|} \hline 0_1, \dots, 0_n & \oplus \\ \hline \end{array}$
 $\varphi^{(1)} = T_1 \oplus s_1$
 $T^{(1)} = \oplus s_1$
 $s_i = 0$
 $s_i = 1$

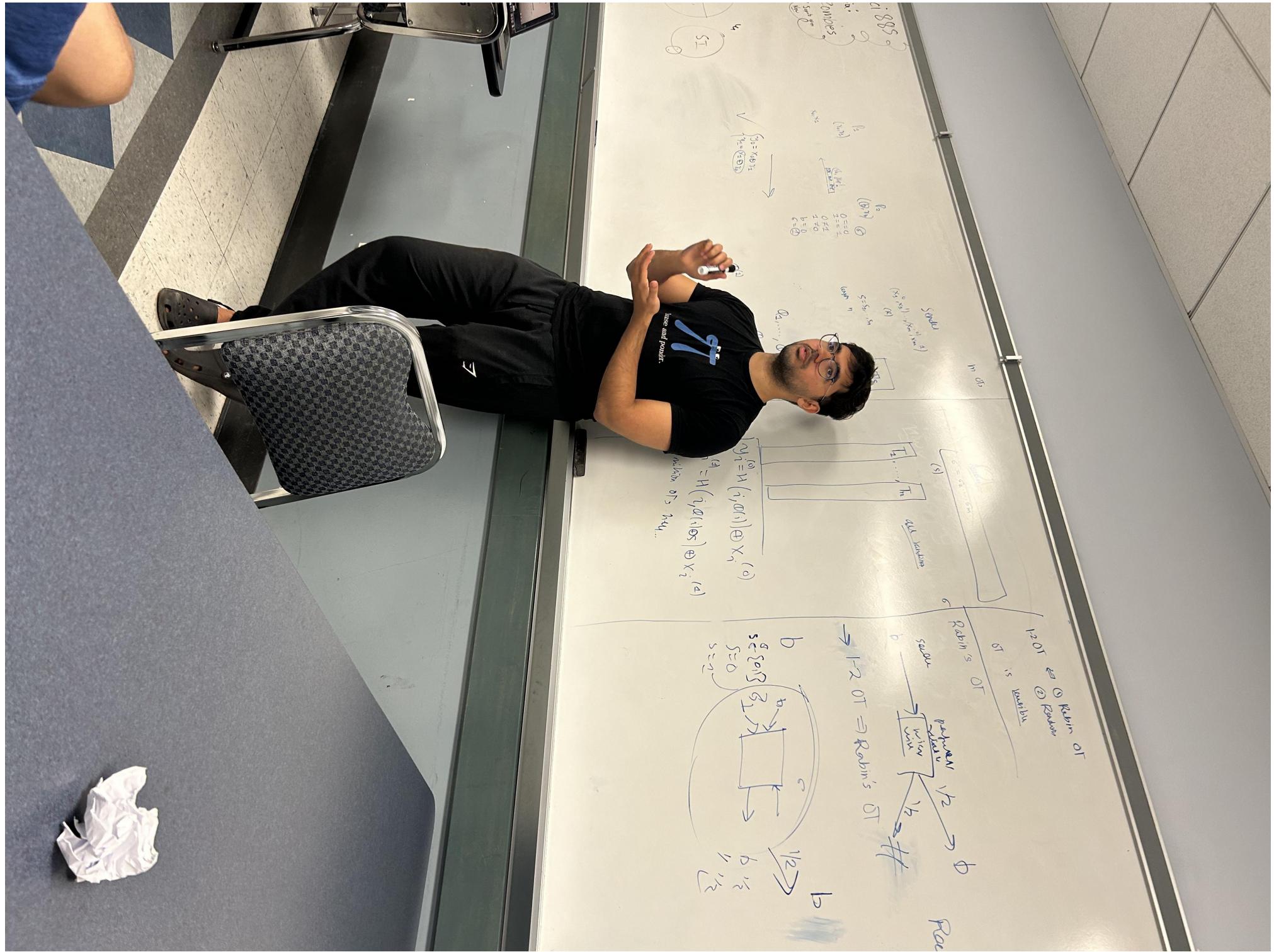
Room: $s = s_1, \dots, s_m$
 (s)
 T_1, \dots, T_m add random

$$\begin{cases} y_1^{(0)} = H(i, \varphi^{(1)}) \oplus x_1^{(0)} \\ y_1^{(1)} = H(i, \varphi^{(1)} \otimes s) \oplus x_1^{(1)} \end{cases}$$

$\Rightarrow \text{million OTs many...}$

$1\text{-}2 \text{ OT} \Leftarrow \begin{array}{l} \textcircled{1} \text{ Rabin OT} \\ \textcircled{2} \text{ Random} \end{array}$
 OT is verifiable
 Rabin's OT
 sender: $b \rightarrow \begin{array}{|c|c|} \hline \text{random value} & b \\ \hline \text{mixer mix} & \oplus \\ \hline \end{array} \rightarrow b'$
 \oplus
 $\rightarrow 1\text{-}2 \text{ OT} \Rightarrow \text{Rabin's OT}$





① Rabin OT

② Rabin

OT is recursive

m OT

Rabin's OT

sender

receiver

public

view

priv

key

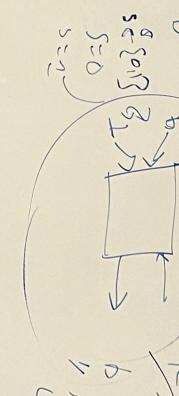
pk

sk

pk'

sk'

b



Receiver

pk

sk

pk'

sk'

pk''

sk''

pk'''

sk'''

pk''''

sk''''

pk'''''

sk'''''

pk''''''

sk''''''

pk'''''''

sk'''''''

pk''''''''

sk''''''''

pk''''''''

sk''''''''

pk'''''''''

sk'''''''''

pk''''''''''

sk''''''''''

pk'''''''''''

sk'''''''''''

pk'''''''''''''

sk'''''''''''''

pk''''''''''''''

sk''''''''''''''

pk''''''''''''''''

sk''''''''''''''''

$$\begin{aligned} Y_{i,1}^{(0)} &= H(i, \sigma_{i,1}) \oplus X_i^{(0)} \\ Y_{i,1}^{(1)} &= H(i, \sigma_{i,1} \parallel \Theta) \oplus X_i^{(1)} \\ &\vdots \\ Y_{i,1}^{(n)} &= H(i, \sigma_{i,1} \parallel \Theta) \oplus X_i^{(n)} \end{aligned}$$

$$\begin{aligned} T_0 &= \sigma_{i,1} \\ T_1 &= \sigma_{i,1} \parallel \Theta \\ T_2 &= \sigma_{i,1} \parallel \Theta \parallel \Theta \\ &\vdots \\ T_n &= \sigma_{i,1} \parallel \Theta \parallel \dots \parallel \Theta \end{aligned}$$

$$\begin{aligned} Y_{i,0} &= Y_{i,1}^{(0)} \parallel T_0 \\ Y_{i,1} &= Y_{i,1}^{(1)} \parallel T_1 \\ &\vdots \\ Y_{i,n} &= Y_{i,1}^{(n)} \parallel T_n \end{aligned}$$

$$\begin{aligned} Y_{i,0} &= Y_{i,1}^{(0)} \parallel T_0 \\ Y_{i,1} &= Y_{i,1}^{(1)} \parallel T_1 \\ &\vdots \\ Y_{i,n} &= Y_{i,1}^{(n)} \parallel T_n \end{aligned}$$