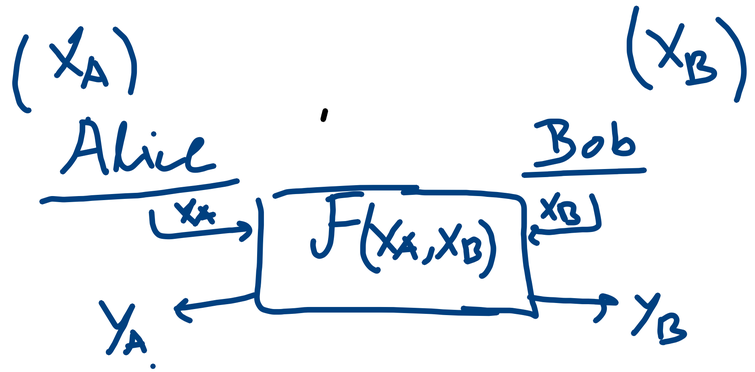


Guarantees:

- Correctness
- Security

$X_A, X_B \in \{0,1\}$

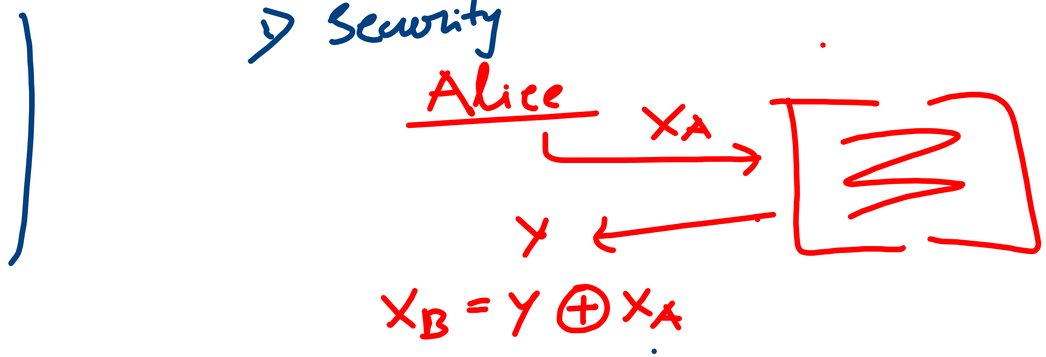
$Y = F_{AND}(X_A, X_B) = X_A \wedge X_B$

Goal:

Security: Knows Y and "nothing else"

eg. $F_{XOR}(X_A, X_B) = X_A \oplus X_B$

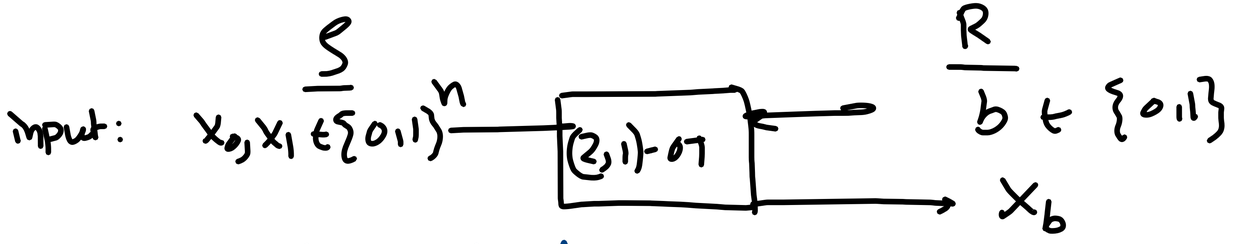
X_A	X_B	Y
0	0	0
0	1	0
1	0	0
1	1	1

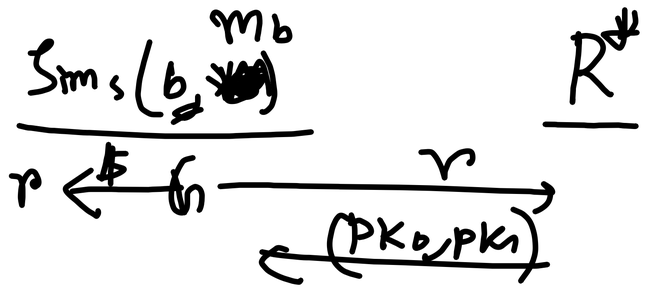


Type of adversaries (Major)

- Semi-honest / passive / honest but curious
- Malicious / Active

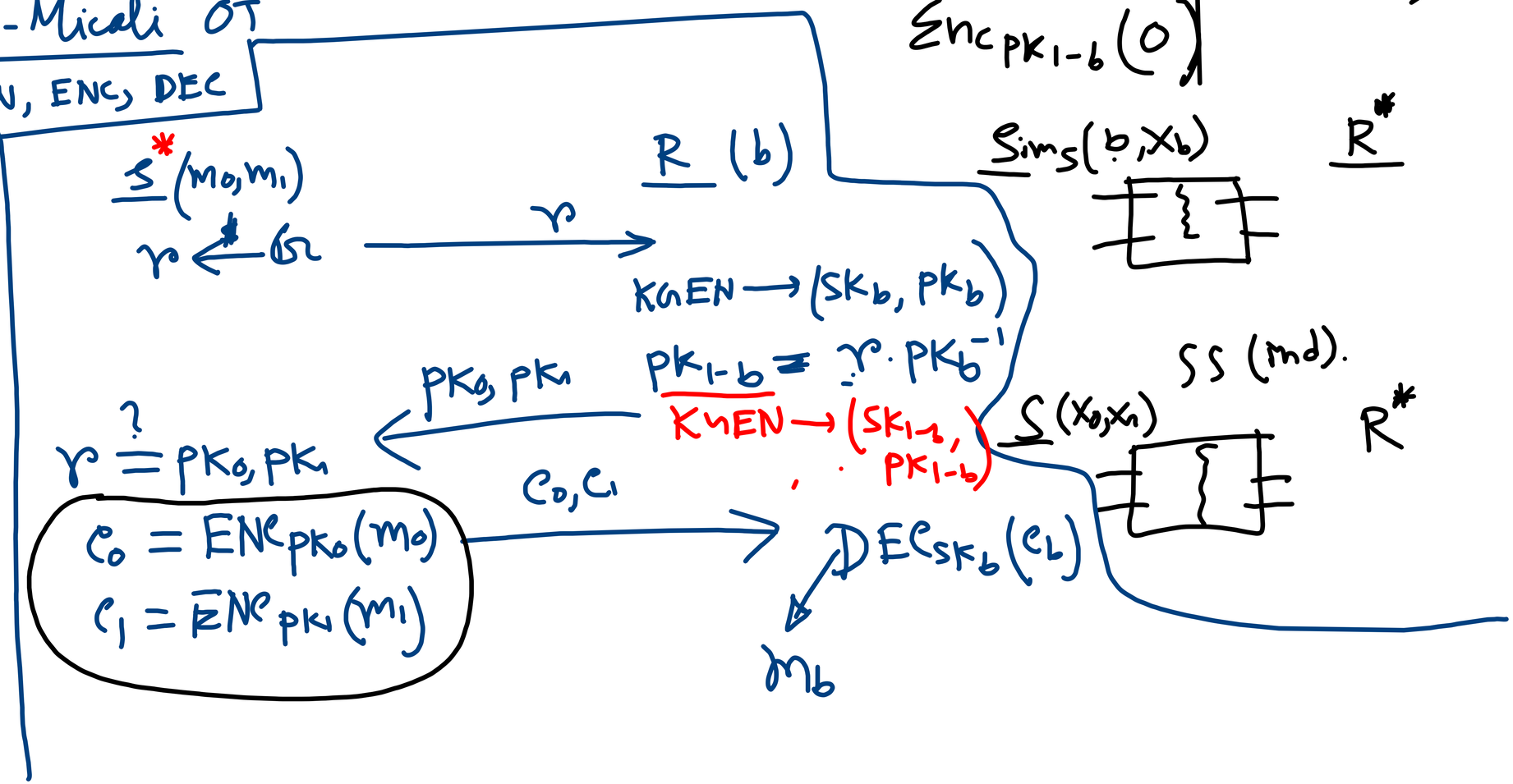
Oblivious Transfer (OT)





Bellare-Micali OT

* PKE = KGEN, ENC, DEC
  - ↓ Dense PK
  - KGEN → (SK, PK)
  - $pk' \xleftarrow{\$} PK$
  - $PK \equiv PK'$
  - e.g. EL-GAMAL
    - $SK \xleftarrow{\$} \mathbb{Z}_p$
    - $pk = g^{SK}$
    - $\langle g \rangle = G$



KGEN, ENC, DEC

S

$(m_{00}, m_{01}, m_{10}, m_{11})$

R

(b_1, b_2)

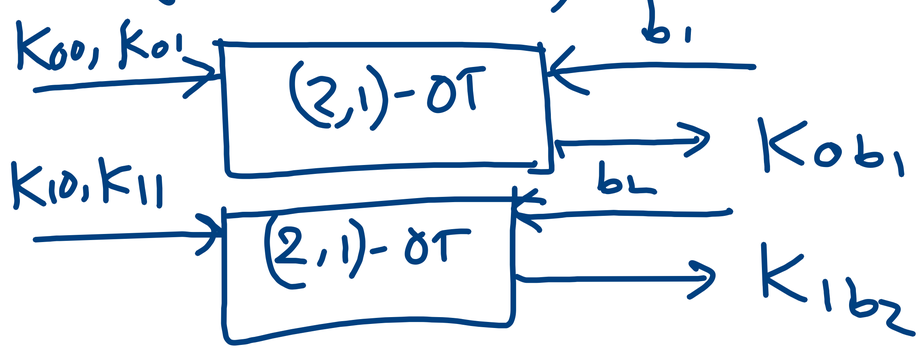
$K_{00}, K_{01}, K_{10}, K_{11} \leftarrow KGEN$

$C_{00} = ENC_{K_{00}}(ENC_{K_{10}}(m_{00}))$

$C_{01} = ENC_{K_{00}}(ENC_{K_{11}}(m_{01}))$

$C_{10} = ENC_{K_{01}}(ENC_{K_{10}}(m_{10}))$

$C_{11} = ENC_{K_{01}}(ENC_{K_{11}}(m_{11}))$



Garbled Circuit (YAO)

(X1) (X2)

Alice $y = x_1 \wedge x_2$ **Bob**

K_1^0 K_2^0 ← {0,1}

K_1^1 K_2^1 ← {0,1}

0 → 0000
1 → 11111
OR 1 invalid

$x_1, x_2 \leftarrow \{0,1\}$

GARBLED GATE (AND)

Permute Randomly

$C_{00} = ENC_{K_1^0}(ENC_{K_2^0}(K_3^0))$

$C_{01} = ENC_{K_1^0}(ENC_{K_2^1}(K_3^0))$

$C_{10} = ENC_{K_1^1}(ENC_{K_2^0}(K_3^0))$

$C_{11} = ENC_{K_1^1}(ENC_{K_2^1}(K_3^1))$

$K_3^0 \rightarrow K_3^0$

$K_3^1 \rightarrow K_3^1$

$K_3^0 \rightarrow K_3^1$

$K_3^1 \rightarrow K_3^1$

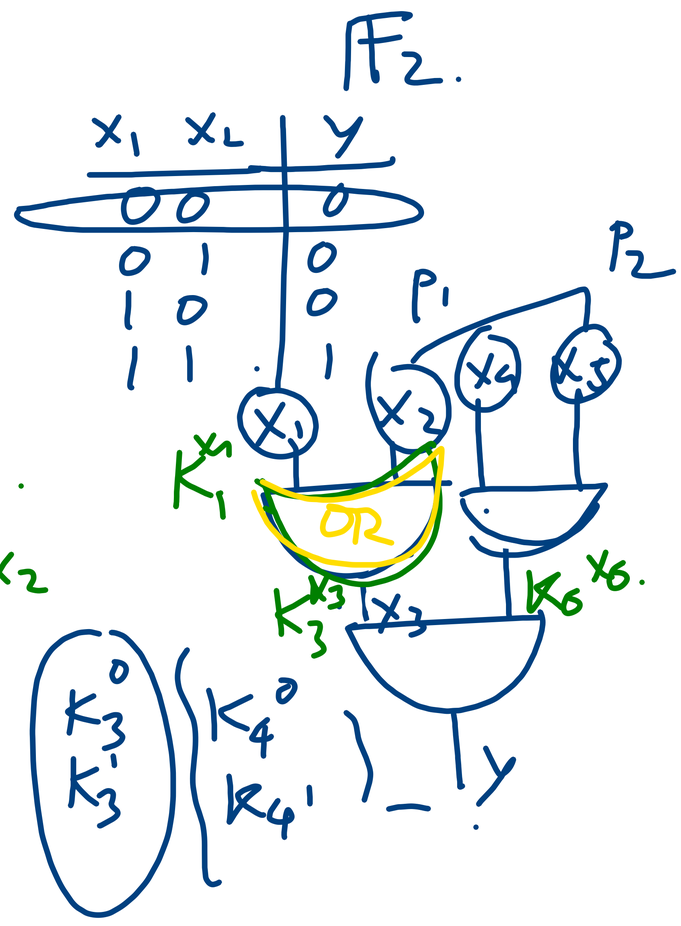
DEC

$C_{x_1 x_2}$

$K_1^{x_1}$

K_2^0, K_2^1 → (2,1)-OT ← x_2

(2,1)-OT → $K_2^{x_2}$



N-party comp

Setting #1: NO HON MAJORITY $\Rightarrow$ At least 1 hon party

Setting #2: HON MAJORITY $\Rightarrow$ $> N/2$ honest parties

N=3 GMW Protocol:

Ingredients

① Additive secret sharing

② (4,1)-OT

over $\mathbb{F}_2$

$a \in \mathbb{F}_2$

Additive sharing among N-parties

$a = a_1 \oplus \cdots \oplus a_N$

$\forall i \in \{1,\ldots,N-1\}\ a_i \xleftarrow{\$} \mathbb{F}_2$

(N-1) shares don't reveal anything

(a) (b) (c)

P_1 P_2 P_3

$a \xrightarrow{\text{Add Sh}} a_1 \oplus a_2 \oplus a_3$

$b \downarrow b_1 \oplus b_2 \oplus b_3$

$c \downarrow c_1 \oplus c_2 \oplus c_3$

a_1, b_1, c_1 $\quad a_2, b_2, c_2$ $\quad a_3, b_3, c_3$

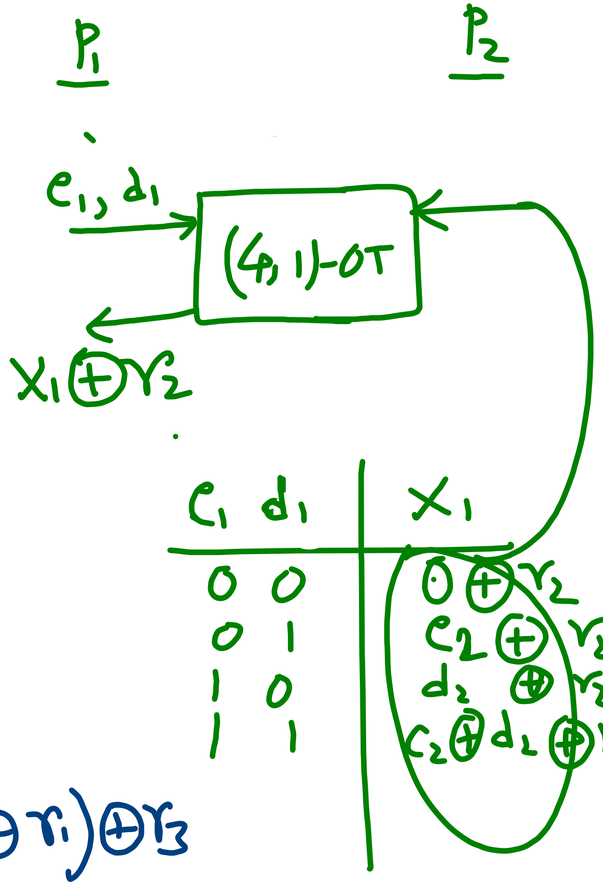
$d_1 = a_1 \oplus b_1$ $\quad d_2 = a_2 \oplus b_2$ $\quad d_3 = a_3 \oplus b_3$

r_1 $\quad r_2$ $\quad r_3$

$y_1 = c_1 d_1 \oplus r_2 \oplus x_1 \oplus r_1$

$y_2 = c_2 d_2 \oplus (x_2 \oplus r_3) \oplus r_2$ (or)

$\bar{y_3} = c_1 d_1 \oplus (x_3 \oplus r_1) \oplus r_3$



BGW protocol (MOD-MAT)

Shamir-Secret-sharing

(t,n)-SSS $\quad t \le n-1$

SHARE $(s) \longrightarrow s_1 \ldots\ldots s_n$

$s \in \mathbb{F}$

$f(x) \xleftarrow{R} \mathbb{F}^t[x]$ s.t. $f(0) = s$

$s_i = f(i)$

RECON $(s_{j_1}, s_{j_2} \ldots\ldots s_{j_{t+1}})$

$$f(0) = s = \sum_{i=1}^{t+1} \lambda_{s,i,0}\, s_{j_i}$$

$S = \{ j_1 \ldots\ldots j_{t+1} \}$

$\mathbb{F}$

↓

arithmetic circuit.

(a) (b) (c) $\begin{pmatrix} t=1 \\ n=3 \end{pmatrix}$

P_1 P_2 P_3

INV: P_i holds (t,n) SSS of each wire

$a \xrightarrow{(t,n)\text{-SS}} a_1, a_2, a_3$ $b \xrightarrow{(t,n)\text{-SS}} b_1, b_2, b_3$ $c \xrightarrow{(t,n)\text{-SS}} c_1, c_2, c_3$

$f_1(1) = a_1$ $f_2(1) = b_1$ $f_3(1) = c_1$

$f_1(2) = a_2$ $f_2(2) = b_2$ $f_3(2) = c_2$

$f_1(3) = a_3$ $f_2(3) = b_3$ $f_3(3) = c_3$

$f_1(0) = a$ $f_2(0) = b$ $f_3(0) = c$

After Rd #1

a_1, b_1, c_1 a_2, b_2, c_2 a_3, b_3, c_3

$d_1 = a_1 + b_1$ $d_2 = a_2 + b_2$ $d_3 = a_3 + b_3$

$= f_1(1) + f_2(1)$ $= f_4(2)$ $= f_4(d_3)$

$= f_4(1)$

$c_1 \cdot d_1 = f_3(1) f_4(1)$ $c_2 d_2 = f_3(2) \cdot f_4(2)$ $c_3 d_3 = \cdots = g(3) = \tilde{e}_3 \xrightarrow{(t,n)\text{-SS}} e_{31}, e_{32}, e_{33}$

$= g(1) = \tilde{e}_1 \xrightarrow{(t,n)\text{-SS}} e_{11}, e_{12}, e_{13}$ $= g(2) = \tilde{e}_2 \xrightarrow{(t,n)\text{-SS}} e_{21}, e_{22}, e_{23}$

h_1 h_2 h_3

P_1 P_2 P_3

e_1 $h(2)$ $h(3)$

$= e_{11} + e_{12} + e_{13} = y_1$ y_1, y_2 $e_{13} + e_{23} + e_{33}$

$h_1(1) + h_2(1) + h_3(1)$ $= y_3$

$= h(1)$ y_3

$h_1 \to h_1(1)\ h_1(2)\ h_1(3)$

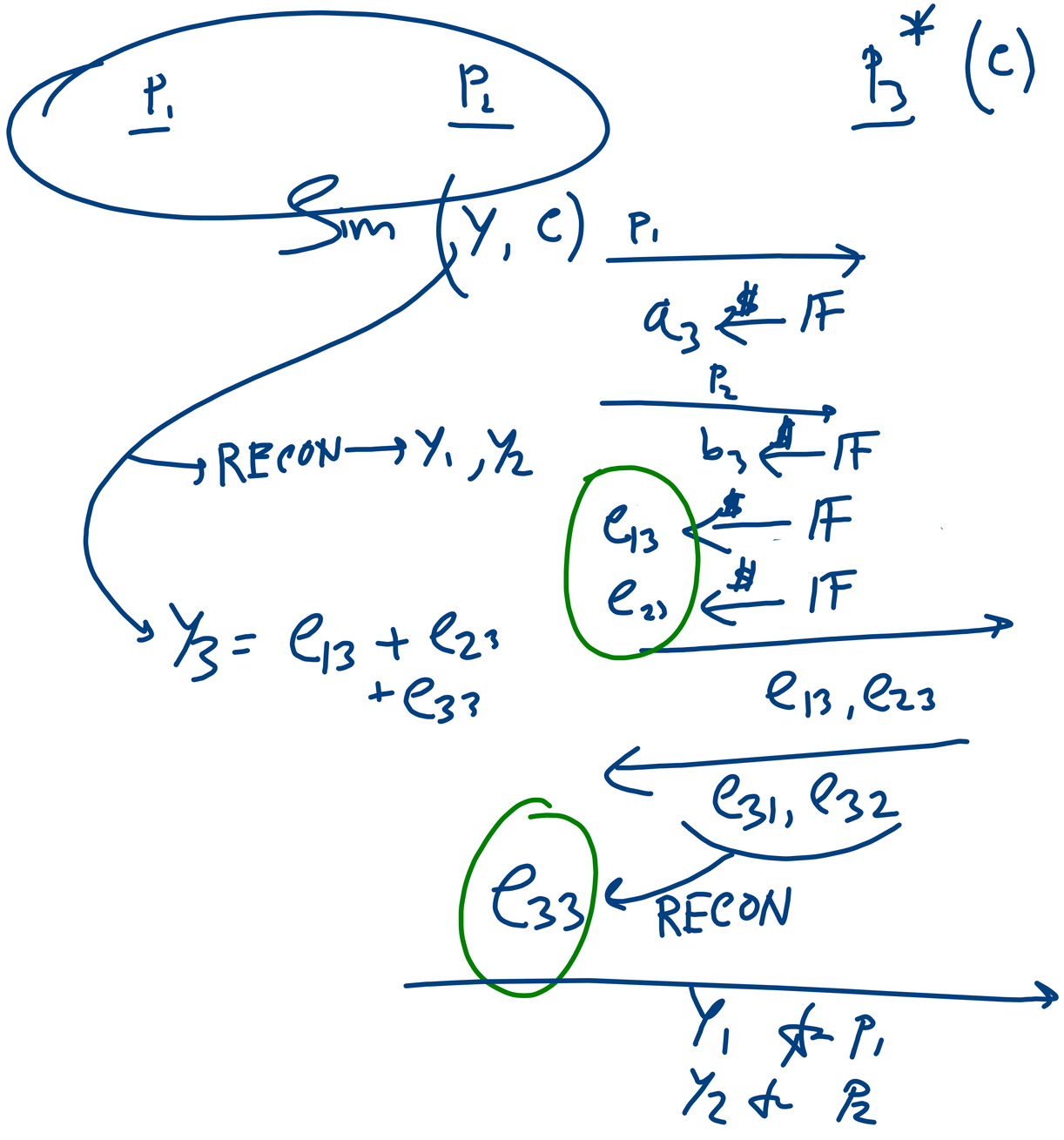
$h_2 \to h_2(1)\ h_2(2)\ h_2(3)$

$h_3 \to h_3(1)\ h_3(2)\ h_3(3)$.

$f_4 \to t\text{-deg}$.

$h_i \to t\text{-deg}$

$g \to 2t\text{-deg}$


P_1
P_2
$P_3^*(C)$
Sim (Y, C)
P_1
a_3 # IF
P_2
b_3 # IF
RECON → Y_1, Y_2
$Y_3 = e_{13} + e_{23} + e_{33}$
e_{13} # IF
e_{23} # IF
e_{13}, e_{23}
e_{31}, e_{32}
e_{33}
RECON
Y_1 ≠ P_1
Y_2 ≠ P_2

Malicious Secrets

Any SH protocol $\xrightarrow{(GMW)}$ Malicious.

P_1 (x_1) — $COM(x_1, rand_1)$ → $H(x_1, r)$

$rand_1 \leftarrow \$$

$MSG_1 = NM_1(x_1, rand_1)$ → P_j

Π_1 → Π_1 VERIFY.