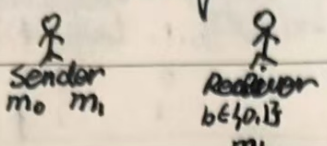
不经意
Oblivious Transfer (OT)



input: Sender m_0 m_1; Receiver $b \in \{0,1\}$
output: Receiver m_b

Random Oblivious Transfer

input: m_0, m_1
output: $b \xleftarrow{\$} \{0,1\}, m_b$

Trapdoor OWP → OT

Sender: F, trapdoor, random Δ
Receiver: $x_b \xleftarrow{\$}$

F, Δ →
$y_0 = F(x_b)$, $y_{1-b} = \Delta - y_0$
← y_0, y_1 s.t. $y_0 + y_1 = \Delta$

$x_0 = F^{-1}(y_0)$, $x_1 = F^{-1}(y_1)$
$c_0 = H(x_0) \oplus m_0$, $c_1 = H(x_1) \oplus m_1$ →

Semi-honest Reciever computationally Secure.
Semi-honest Sender Perfectly Secure.

← Enc(b)
Enc(m_b) →

Oblivious Linear Function Evaluation (OLE)

input: Sender $a, b \in \mathbb{F}$; Receiver $x \in \mathbb{F}$
output: $ax+b \in \mathbb{F}$

Dallior → OLE

public parameter
public parameter: N^2, g, h

Sender a, b — Receiver x

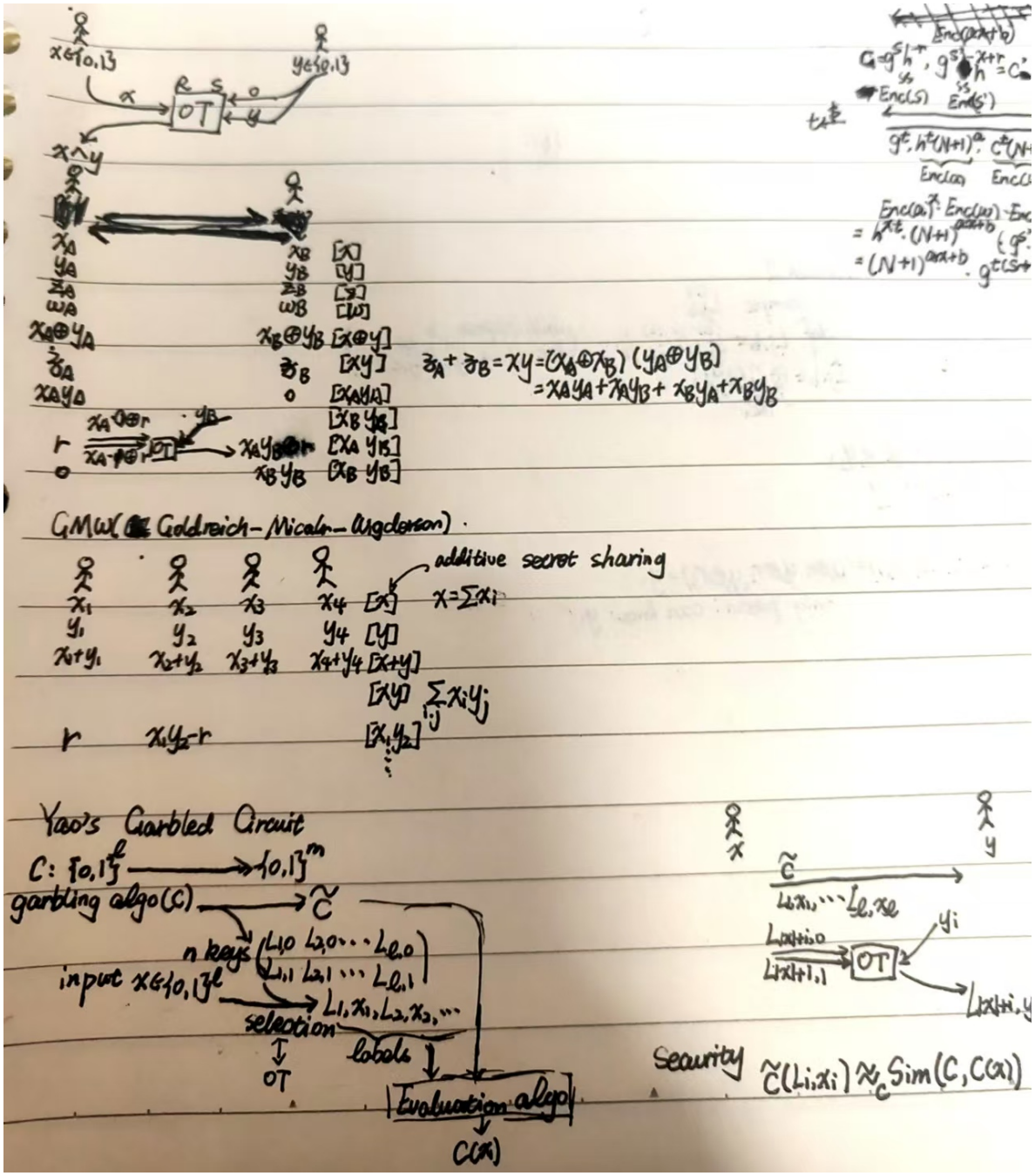
← Enc(x)
$s, s', r \xleftarrow{\$}$
Enc($ax+b$) →

$c_1 = g^{s} h^{r}$, $g^{s'} h^{-x+r} = c_0'$

← Enc(s) Enc(s')
$t \xleftarrow{\$}$
$g^t, h^t(N+1)^a \cdot c^t(N+1)^{\omega} \cdot (c')^t(N+1)^{b-\omega}$

Enc(a) Enc(ω) Enc(b−ω)

$\text{Enc}(a)^x \cdot \text{Enc}(\omega) \cdot \text{Enc}(b-\omega)$
$= h^{xt} \cdot (N+1)^{ax+b} \cdot (g^{s'} h^{r-x} \cdot g^{s} h^{-r})^t$
$= (N+1)^{ax+b} \cdot g^{t(s+s')}$


OT
GMW (Goldreich-Micali-Wigderson)
additive secret sharing
Yao's Garbled Circuit
garbling algo(C)
n keys
input
selection
labels
OT
Evaluation algo
C(x)
Security

Yao's Garbled Circuit

Table

$Enc(L_{i,0}, Enc(L_{j,0}, L_{k,g(0,0)}))$			
$Enc(L_{i,0}, Enc(L_{j,1}, L_{k,g(0,1)}))$			
	1	0	0
	1	1	1

shuffle

$Enc(L_{k,0}, 0^n \| 000)$
$Enc(L_{k,1}, 0^n \| 000)$

permute bit α_i
color bit $\tilde{x}_i = \alpha_i \oplus x_i$

0	0	$\alpha_i \; \alpha_j$
0	1	$\alpha_i \; \alpha_j \oplus 1$
1	0	$\alpha_i \oplus 1 \; \alpha_j$
1	1	$\alpha_i \oplus 1 \; \alpha_j \oplus 1$

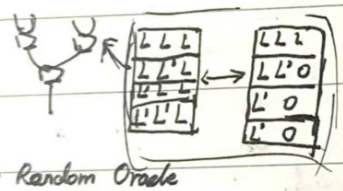
real world

Simulator

(left right output)

$Enc(L, Enc(L_2, L))$
$Enc(L, Enc(L', L))$
$Enc(L', 0)$
$Enc(L', 0 \cdots 0)$

$Enc(L_{i,b})$
$Enc(L_{i,\bar{b}})$



under Random Oracle

$H(L, L) \oplus L$
$H(L, L') = h_2 \oplus L$
$H(L', L) = h_3 \oplus L$
$H(L', L') = h_4 \oplus L$

Approach I

P_i sample $L_{j,b}^{(i)}$
def $L_{j,b} = \bigoplus_{i=1}^{n} L_{j,b}^{(i)}$

Approach II

P_i sample $L_{j,b}^{(i)}$
def $L_{j,b} = L_{j,b}^{(1)} \| L_{j,b}^{(2)} \| \cdots$ (will expose b
(let $L_{j,c} = L_{j,c}^{(1)} \| L_{j,c}^{(2)} \| \cdots$)
$\hat{L}_{j,b} = \bigoplus_i G_i(L_{j,b}^{(i)})$
PRG

MPC for $F(x_1, x_2, x_3) = (y_1, y_2, y_3)$
MPC for $F(x_1, x_2, x_3) = y$.
"$\Rightarrow$" obviously
"$\Leftarrow$" let $F((x_1, r_1), (x_2, r_2), (x_3, r_3)) = (y_1 \oplus r_1, y_2 \oplus r_2, y_3 \oplus r_3) = y$.
only person i can know y_i