- lectures will be recorded & available on ELMS
- Sign up for Piazza

Theorem

For any n-input functionality F, there is an n-party protocol that $(n-1)$-securely computes F (for semi-honest adversaries), assuming semi-honest OT.

Proof [GMW protocol] Goldreich-Micali-Wigderson '87

- Work in OT-hybrid model
  - protocol is perfectly secure in OT-hybrid model
- Consider deterministic functions
  - can reduce randomized functionalities to this case

1) Input-sharing phase:

Assume P_i holds input bit x

P_i chooses $x_2, \ldots, x_n \leftarrow \{0,1\}$

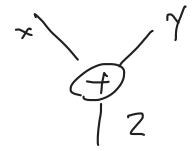
set $x_1 = x \oplus x_2 \oplus \ldots \oplus x_n$

send share x_i to P_i

2) Circuit evaluation:

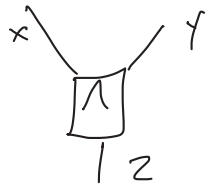
- Parties begin holding $x_1, \ldots, x_n$ s.t. $\bigoplus_{i=1}^{n} x_i = x$
- P_1 sets $y_1 = \bar{x}_1$

  P_i, $i \neq 1$ sets $y_i = x_i$



- Parties begin holding shares of x, y, i.e.,
  P_i holds x_i, y_i s.t. $\bigoplus x_i = x$, $\bigoplus y_i = y$
- P_i sets $z_i = x_i \oplus y_i$

  Check: $\bigoplus z_i = \bigoplus (x_i \oplus y_i) = (\bigoplus x_i) \oplus (\bigoplus y_i) = x \oplus y$



- Parties begin holding shares of x, y

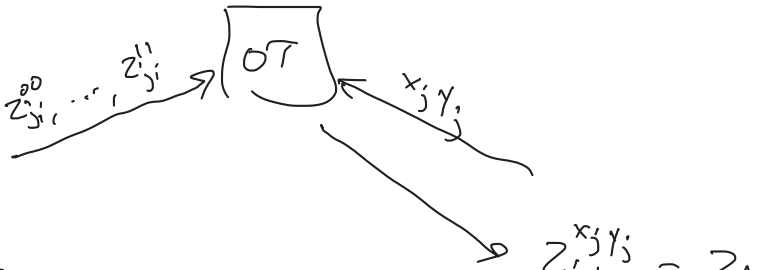
  Want to compute shares of $z = (x_1 \oplus \cdots \oplus x_n) \cdot (y_1 \oplus \cdots \oplus y_n)$

$$\Rightarrow z = \bigoplus_{i,j} x_i y_j = \left(\bigoplus_i x_i y_i\right) \oplus \left(\bigoplus_{i<j} (x_i y_j \oplus x_j y_i)\right)$$

$i < j$

$P_i(x_i, y_i)$ $P_j(x_j, y_j)$ $x_i y_j \oplus x_j y_i$

$z_{ij} \leftarrow \{0,1\}$



if $x_j = 0, y_j = 0$
$z_{ji}^{00} = z_{ij}$

if $x_j = 0, y_j = 1$
$z_{ji}^{01} = z_{ij} \oplus (x_i)$

if $x_j = 1, y_j = 0$

if $x_j = 1, y_j = 1$
$z_{ji}^{11} = z_{ij} \oplus (x_i \oplus y_i)$

z_{ij} z_{ji} $z_{ij} \oplus z_{ji} =$
$x_i y_j \oplus x_j y_i$

P_i sets $z_i = x_i y_i \oplus \left(\bigoplus_{j \neq i} z_{ij} \right)$

Now $z_1 \oplus z_2 \oplus \cdots \oplus z_n = z$

---

3) Output reconstruction

if output wire γ should be learned by P_i
then all parties send shares of γ to P_i

GMW '87 — relies on OT, $(n-1)$-security

BGW '88, CCD '88 — unconditional, $t < n/2$ security } semi-honest

GMW '87 - OT + ZK, $(n-1)$-secure

BGW '88, CCD '88 - unconditional, $t < n/3$ security } malicious

Rabin-BenOR '89, Beaver '89

- unconditional, $t < n/2$ security, broadcast

Efficiency of semi-honest GMW protocol?

- evaluate all AND gates at the same level in parallel
- round complexity is $O(d)$, where d is the depth of the circuit computing F
- Computation/Communication (ignoring OT protocol) very low
- $O(n^2 \cdot |C|)$ oblivious transfers
  - Can # of OTs be reduced?

What's next?

- Improved round complexity?
- Statistical security (w/o OT)?
- Malicious security?

Yao's garbled circuit approach

Theorem [Yao '86]

Assuming semi-honest OT & secure private-key encryption, there is a constant-round protocol computing any 2-party function f (in the semi-honest setting).

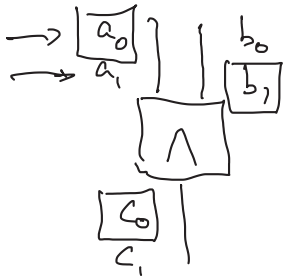
Proof

$P_1(x)$ $\qquad$ $P_2(y)$

$f \longrightarrow GC_f$

$GC_f \longrightarrow$

$a, b \Rightarrow a \wedge b$



$a_x, b_y \Rightarrow c_{x \wedge y}$

Garbled gate:

randomly permute

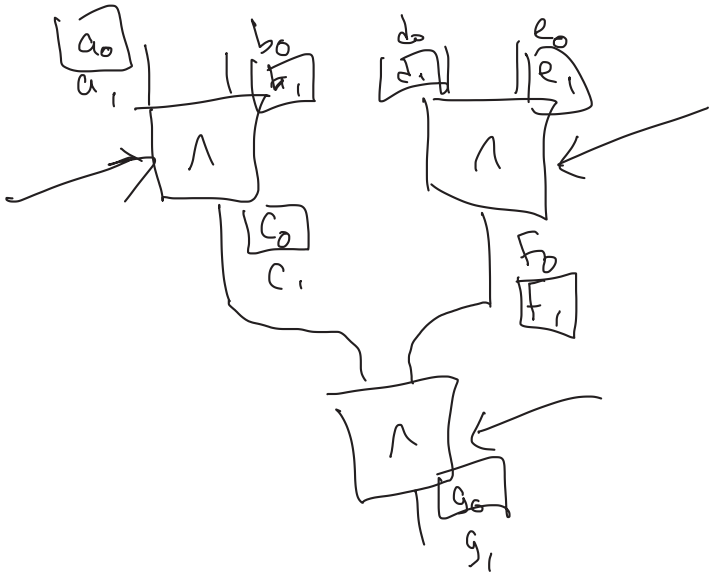
$Enc_{a_0}(Enc_{b_0}(c_0))$	row_{00} ✗
$Enc_{a_0}(Enc_{b_1}(c_0))$	row_{01} ✗
$Enc_{a_1}(Enc_{b_0}(c_0))$	row_{10} ✓
$Enc_{a_1}(Enc_{b_1}(c_1))$	row_{11}

regular gate

a \ b	0	1
0	0	0
1	0	1

garbled gate

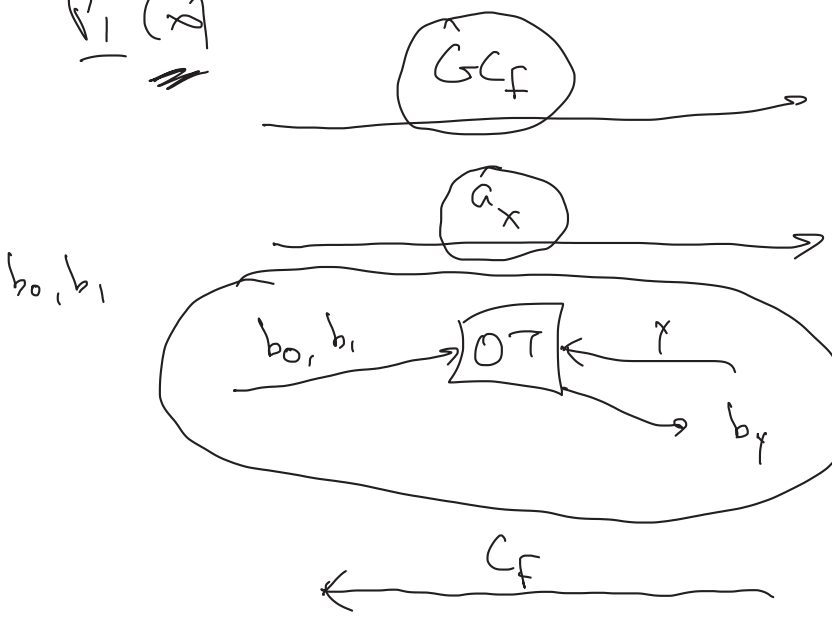
	a_0	a_1
b_0	c_0	c_0
b_1	c_0	c_1



$$f(a,b,c,d) = (a \wedge b) \wedge (c \wedge d)$$

GC_f : given keys for the input wires (one key per wire) corresponding to inputs $x_1, \ldots, x_n \in \{0,1\}^*$, can evaluate GC_f to get keys on the output wires (one key per wire) corresponding to $F(x_1, \ldots, x_n)$

$P_1(x)$



$P_2(y)$

evaluate circuit to $C_f(x,y)$