finishing up real-ideal paradigm & Garbled Circuits

Last time:

**Real interaction**

\[ \begin{array}{c}
A \\
\downarrow \pi \quad \Leftrightarrow \quad \downarrow l \\
B
\end{array} \]

**Ideal Interaction**

\[ \begin{array}{c}
S \\
\downarrow x \\
\quad f(x,y) \\
\quad \quad f(x,y) \\
B \quad \quad \downarrow y
\end{array} \]

**Security definition:**

for all adversaries A attacking real interactions

there exists an adv/simulator S attacking ideal interaction

that achieve "same effect" for all input distributions

**Semi-honest adversaries:** runs the protocol, outputs its view

"achieves same effect" = simulate Adversary's view

(given only \(x\), \(f(x,y)\))

**Malicious adversaries:** can deviate arbitrarily from protocol

"effect" of an adversary is (A's view, B's output)

suppose A can make Bob output \(z\).

If this is possible in ideal interaction too, then not an "attack"

**Note:** "malicious simulator" can choose input to \(f\) arbitrarily (semi-honest must use \(x\) that was given)
Ex: XOR protocol

\[ \begin{array}{c}
\text{A} \\
\downarrow
\end{array} \xrightarrow{x \oplus y} \begin{array}{c}
\text{B} \\
\downarrow
\end{array} \xrightarrow{z}
\]

It is semi-honest secure (can simulate both parties' views).

It is not secure against malicious adversaries.

Attack idea #1:

\[ \begin{array}{c}
\text{A} \\
\downarrow
\end{array} \xrightarrow{x \oplus y} \begin{array}{c}
\text{B} \\
\downarrow
\end{array} \xrightarrow{z}
\]

Send complement of your input? Not an attack, because same effect can be achieved in ideal world by sending \( \bar{x} \).

Idea #2:

\[ \begin{array}{c}
\text{A} \\
\downarrow
\end{array} \xrightarrow{y} \begin{array}{c}
\text{B} \\
\downarrow
\end{array} \xrightarrow{z = 0}
\]

Can't achieve this effect in ideal world, when Bob's input random.

\[ \Pr[\text{Bob output 0}] = \frac{1}{2} \quad \text{vs.} \quad \Pr[x \oplus y = 0] = \frac{1}{2} \]

Garbled circuits:

Circuits: wires, contain 0 or 1
Input wires / output wires
Gates computing \( G: \{0, 1\}^2 \rightarrow \{0, 1\} \)
Acyclic, directed
is $x_1 x_0 > y_1 y_0$?

**Ex:**

```
<table>
<thead>
<tr>
<th>A0, x1</th>
<th>E0, E1</th>
</tr>
</thead>
<tbody>
<tr>
<td>B0, y0</td>
<td>E0, E1</td>
</tr>
<tr>
<td>C0, s1</td>
<td>E0, E1</td>
</tr>
<tr>
<td>D0, d1</td>
<td>H0, H1</td>
</tr>
</tbody>
</table>
```

**Idea:** for every wire, pick 2 “keys”/“labels” from $\{0, 1\}$

to represent $T$ & $E$

( $A_0$ = false, $A_1$ = true)

for each gate, generate 4 ciphertexts

**Ex:**

```
I0 I1
<table>
<thead>
<tr>
<th>E0, E1</th>
</tr>
</thead>
<tbody>
<tr>
<td>H0 H1</td>
</tr>
</tbody>
</table>
```

```
Enc(E0, Enc(H0, I0))
Enc(E0, Enc(H1, I1))
Enc(E1, Enc(H0, I1))
Enc(E1, Enc(H1, I2))
```

if you know only 1 of the 2 wire labels on each wire, then only 1 way to proceed

(learn only 1 label on output wire)