Lecture 23
Outline

Garbled Circuits: Security

Q & A from Homework
Garbled Circuits: Security

$$(C, \tilde{a})$$

$${\text{Enc}}_{K_1}, {\text{Enc}}_{K_2}(K?)$$

$${\text{Enc}}_{K_3}(?)$$

$${\text{C}}(a, b)$$
Garbled Circuits: Security
Garbled Gate: Security

\[ \text{Sim}(b, z) : (\text{Garbled Table } G, \text{ Keys, output map}) \]

where \( z = \mathcal{G}(a, b) \)
AND. \( K_a, K_b \rightarrow K \)

<table>
<thead>
<tr>
<th>0 0</th>
<th>0 1</th>
<th>1 0</th>
<th>1 1</th>
</tr>
</thead>
</table>

formulas:
- \( E_{ka,0}(E_{kb,0}(K_0)) \)
- \( E_{ka,0}(E_{kb,1}(K_0)) \)
- \( E_{ka,1}(E_{kb,0}(K_0)) \)
- \( E_{ka,1}(E_{kb,1}(K_1)) \)

\[ a = 0 \Rightarrow \text{Send } K_{a,0} \]

Use OR to transmit

1 out of \( K_{b,0}, K_{b,1} \) to Bob.

Bob's input \( b = 1 \) (w.l.o.g.)

---

**Game 1**

Same as Alice's interaction with Bob, except invoke OT simulator to learn Bob's input \( b \) to Sim.

**Claim 1:** Bob's view in interaction with Alice \n\n\sim Bob's view in Game 1 [OT simulation security]

---

**Game 2**

Same as Game 1, except...

- \( E_{ka,0}(E_{kb,1}(K_0)) \)
- \( E_{ka,0}(E_{kb,0}(K_0)) \)
- \( E_{ka,1}(E_{kb,0}(K_0)) \)
- \( E_{ka,1}(E_{kb,1}(K_1)) \)
Claim 2: Bob's view in Game 1 \( \cong \) Bob's view in Game 2.

\[ \forall \text{PPT } \mathcal{A}, \quad \Pr[\mathcal{A}(\cdot)=1] - \Pr[\mathcal{A}(\cdot)=1] = \neg \text{negl.} \]

Proof: Suppose not. Then \( \mathcal{W} \) that contradicts CPA-security of our encryption scheme.

\( \mathcal{W} \) submits to CPA ch.

- \( m_0 \leftarrow E_{Kb,1}(K_1) \)
- \( m_1 \leftarrow E_{Kb,1}(0, \ldots, 0) \)

Obtains

\[
\begin{align*}
E_{K_a,1}(m_d), & \quad E_{K_b,1}(E_{K_b,0}(K_0)) \\
C^* & \quad C^{**}
\end{align*}
\]

If \( d = 0 \), Game 1

\( d = 1 \), Game 2.

Game 3:

Bob obtains

\( K_a,0, K_b,1 \).

Claim 3: Bob's view in Game 2 \( \cong \) Bob's view in Game 3.
Claim 4: Bob's view in Game 3 \sim Bob's view in Game 4.

Note: Game 4 is identical to Simulator's output up to renaming $K_{a,0} \rightarrow \overline{K}$

\[
\begin{align*}
K_0 & \rightarrow K_{out} \\
K_{b,1} & \rightarrow \overline{K} \\
K_0 & \rightarrow K_{out}
\end{align*}
\]