Outline

Garbled Circuits

Security
Garbled Circuits

\[ C(a, b) \]
Garbled Gate

Garbled Table

<table>
<thead>
<tr>
<th>w1</th>
<th>w2</th>
<th>w5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

out of \((K_o^2, K_i^2)\) Alice wants to send \(K_b^2\) to Bob where \(b\) is Bob’s choice bit

\(C(a, b)\)

\(k_o^5, 0\)

\(k_i^5, 1\)
Garbled Circuit

CORRECTNESS.
Garbled Circuit: Security

$C(a, b)$

$\overline{K, \overline{K, K, K, K}}$

$\begin{array}{c}
K_0 \\
K_1 
\end{array}$
Garbled Gate: Security

\[
\begin{array}{c}
\text{Enc } K_0^1 \quad \text{Enc } K_0^2 \quad \text{Enc } K_0^3 \quad \text{Enc } K_0^4 \quad \text{Enc } K_0^5 \\
\hline
K_0^1 \quad K_0^2 \quad K_0^3 \quad K_0^4 \quad K_0^5
\end{array}
\]

Randomly permuted

\[
K_a^1, K_b^2, K_c^3
\]

\[
\begin{array}{c|c}
K_0^1 & 0 \\
K_0^2 & 1
\end{array}
\]

via OT
Garbled Gate: Security

Sample $k_5, k_5'$ at random.

Simulated Garbled Table

\[
\begin{array}{ccc}
   \text{Enc}_K(\text{Enc}_{k_5}(0)) & \text{Enc}_K(\text{Enc}_{k_5'}(0)) & \text{Enc}_K(\text{Enc}_{k_5'}(1)) \\
   \text{Enc}_K(\text{Enc}_{k_5}(1)) & \text{Enc}_K(\text{Enc}_{k_5'}(0)) & \text{Enc}_K(\text{Enc}_{k_5'}(0)) \\
   \end{array}
\]

Sdp map

\[
\begin{array}{c|c}
   k_5 & 0 \\
   k_5' & 1 \\
\end{array}
\]

Send these keys:

C(a,b) = 1

H.W.: reduce to CPA security.
Garbled Gate: Security
Garbled Circuit: Security
Garbled Circuit: Security
Garbled Circuit: Security