Malicious 2PC based on garbled circuits

- Use OT protocol secure against malicious adversaries
- \( P_i \) can violate correctness by garbling the wrong circuit, or swapping OT inputs
- Can lead to violations of privacy
- Selective-failure attack on privacy

Case 1: \( P_i \) does selective-failure attack on at most 1 wires
\( \Rightarrow \) leaks nothing about \( x \)

Case 2: \( P_i \) does selective-failure attack on all \( n \) wires
\( \Rightarrow \) for one value of \( x \)
- \( P_i \) always aborts
- For other value of \( x \), \( P_i \) aborts except \( \omega/ \text{prob } 2^{-n} \)
Cut-and-choose

\[ P_1 \]

\[ \overline{01} \]

\[ P_2 \]

\[ G_{c_1}, G_{c_2}, \ldots, G_{c_s} \rightarrow S \subseteq \{1, \ldots, 2^k\}, |S| = \frac{k}{2} \]

Open garbled circuit in \( S \), check circuits in \( S \), and abort if any are incorrect.

\( P_1 \) maximizes its prob. of successfully cheating if \( \frac{k}{2} \) circuits are bad.

\[
P_c(\text{succ}) = \frac{\binom{2^k}{\frac{k}{2}}}{\binom{2^k}{\frac{k}{2}}} = \frac{(2^k)! \cdot \frac{k}{2}!}{\frac{k}{2}! \cdot \left(2^k - \frac{k}{2}\right)!} \\
= \frac{(2^k) \cdots (2^k + \frac{k}{2} - 1)}{\frac{k}{2} \cdots \left(\frac{k}{2} + \frac{k}{2} - 1\right)} \leq 2^{-\frac{k}{4}}
\]

So for prob of cheating \( 2^{-n} \Rightarrow 2^k \leq 4n \) (this can be improved to \( k \geq 3n \))

Optimization:

generate \( G_{c_1}, \ldots, G_{c_s} \) from \( k \),

\[ H(G_{c_1}), \ldots, H(G_{c_s}) \rightarrow S \]

\[ \forall i \in S, \text{send } K_i; \]

\[ \forall i \in S, \text{send } G_{c_i}; \]

regenerate \( G_{c_i} \) from \( K_i \), check the hash.

\[ \text{check the hash.} \]
Cut-and-choose can be done w/ in garbled circuits

LECS approach: cut-and-choose on gates

Choose some fraction to check

Check...

For security $2^{-n}$, the total of garbled gates needed is $O\left(\frac{cl \cdot n}{\log c}\right)$

Let $2W$ be total # of garbled gates, say B are bad, say $P_2$ checks half the gates, let $2W+1$ be # of gates in supergate

$P = P_s \leq 2^{-B \cdot \frac{1}{c}} \cdot \frac{B}{n} \cdot \frac{1}{c} \Rightarrow \Pr\left[P_1 \text{ succeeds}\right] \leq O\left(\frac{1}{c^2}\right)$

Setting $\ell = \Theta(n / \log c)$ gives security $2^{-\Theta(n)}$

prob. some fixed super-gate has majority bad gates

prob. no bad gates are checked

union bound over (super) gates