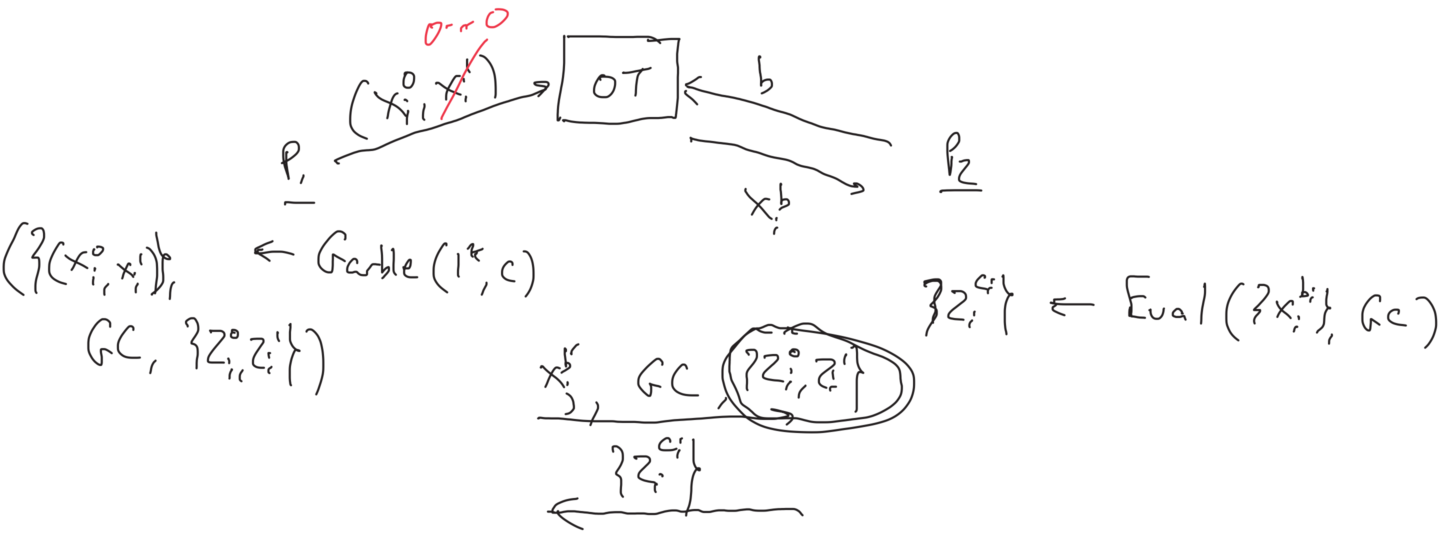
- Scribes?
- lecture recording

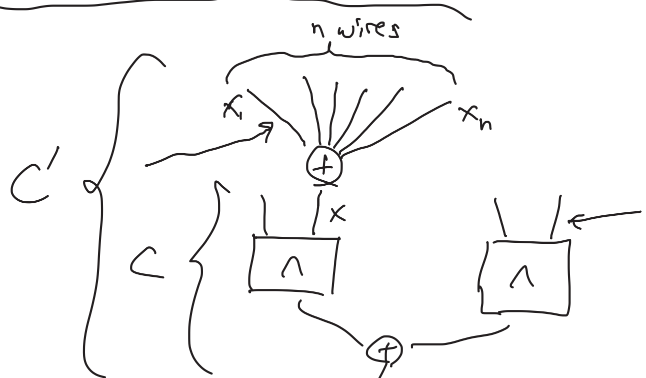
Malicious 2PC based on garbled circuits



- Use OT protocol secure against malicious adversaries
- P_1 can violate correctness by garbling the wrong circuit, or swapping OT inputs
- -- can lead to violations of privacy
- selective-failure attack on privacy

Preventing selective-failure attack:

$\oplus x_i = x$



Case 1: P_1 does selective-failure attack on $\le n-1$ wires
$\Rightarrow$ leaks nothing about x

Case 2: P_1 does selective-failure attack on all n wires
$\Rightarrow$ for one value of x, P_2 always aborts
for other value of x, P_2 aborts except w/ prob 2^{-n}

Cut-and-choose

OT

P_1 $\qquad\qquad\qquad$ P_2

$GC_1, GC_2, \ldots, GC_\ell \longrightarrow$

$\longleftarrow S \subseteq \{1, \ldots, \ell\}, \ |S| = \ell/2$

Open garbled circuits in S $\longrightarrow$ $\qquad$ check circuits in S, and abort if any are incorrect

evaluate garbled circuits not in S

take majority vote on every output wire

P_1 maximizes its prob. of successfully cheating if $\ell/4$ circuits are bad

$$\Pr(\text{succ}) = \frac{\binom{3\ell/4}{\ell/2}}{\binom{\ell}{\ell/2}} = \frac{(3\ell/4)!\,(\ell/2)!}{(\ell/4)!\,\ell!}$$

$$= \frac{(\ell/2)\cdots(\ell/4+1)}{\ell\cdots(3\ell/4+1)} \le 2^{-\ell/4}$$

So for prob of cheating $2^{-n} \Rightarrow \ell \approx 4n$ (this can be improved to $\ell \approx 3n$)

Optimization:

generate GC_i from k_i $\qquad$ $H(GC_1), \ldots, H(GC_\ell) \longrightarrow$

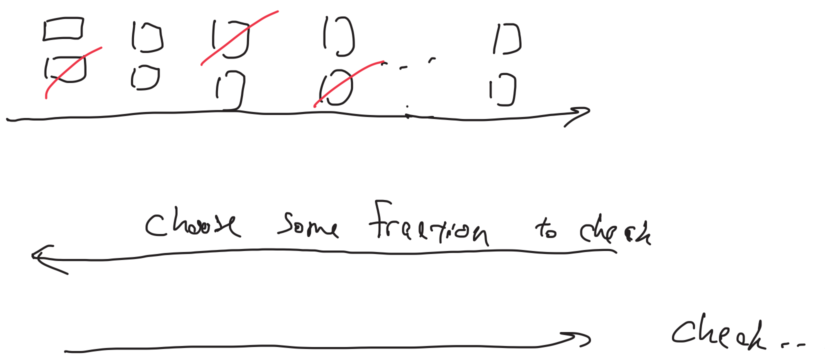
$\longleftarrow S$

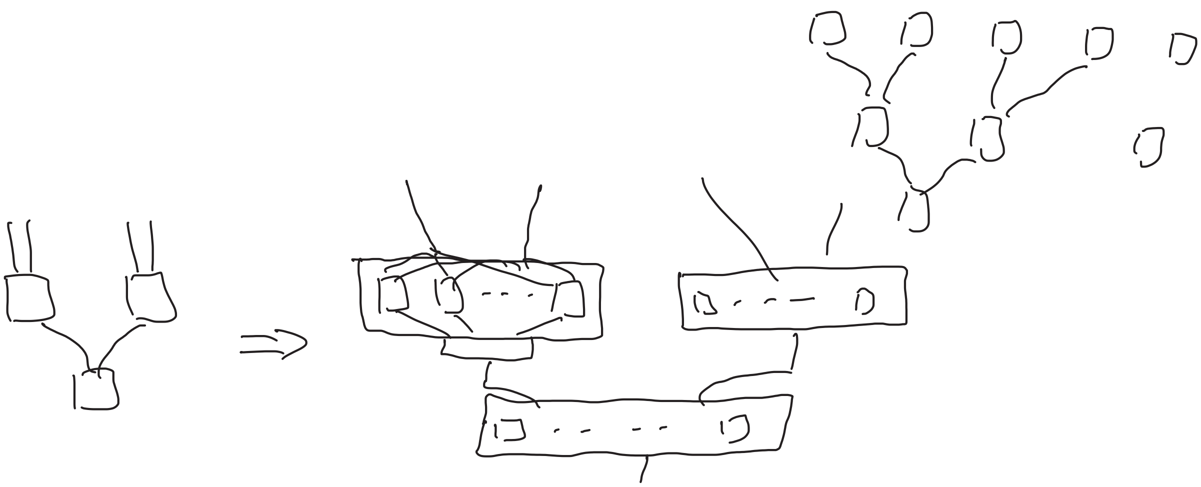
$\forall i \in S$, send k_i $\longrightarrow$ $\qquad$ regenerate GC_i from k_i, & check the hash

$\forall i \notin S$, send GC_i $\qquad$ check the hash

Cut-and-choose can be done w/ n garbled circuits

LEGO approach: cut-and-choose on gates





For security 2^{-n}, the total of garbled gates needed is $O(|C| \cdot n / \log |C|)$

let $2N$ be total # of garbled gates, say B are bad,

say P_2 checks half the gates, let $2l+1$ be # of gates in supergate

$$\Pr[P_1 \text{ succeeds}] \leq 2^{-B} \cdot |C| \cdot \underbrace{\left(\frac{B}{N}\right)^{l+1} \cdot 2^{2l}}_{\text{prob. some fixed supergate has majority bad gates}} \Longrightarrow \Pr[P_1 \text{ succeeds}] \leq O\left(\frac{1}{C^l}\right)$$

setting $l = \Theta(n / \log C)$ gives security $2^{-\Theta(n)}$

prob. no bad gates are checked

union bound over (super) gates

prob. some fixed supergate has majority bad gates