1 Summary

In this lecture we introduced a much more efficient protocol for malicious security given a weaker notation of security. In particular, we talk about efficient GC under 1-bit leakage[1].

In general, we define security by comparing real world to ideal world. When we say a weaker security, we can do the followings:

- Weaken the notation of "comparison"
- Weaken the ideal world
  - 1-bit leakage
  - covert security

**weaker model of security** The malicious party can send a function $g()$ and get $g(x)$ when receiving result from ideal functionality.

2 The protocol for 1-bit-leakage

The protocol is as follows, where $Z^b_i$ is the label for $i$-th output wire when the value is $b$. 
3 Proof using simulation

WLOG, we assume that P2 is corrupted and we have simulator S:

1) Extract P2’s input to OT in first phase ⇒ this defines input $y$

2) send $y$ to ideal functionality and get back $v$
3) use semi-honest simulation to generate all input-wire labels, Garbled Circuits, to give to P2. We also output \( \{Z_i^{v_i}\}_{i=1}^n \). We choose uniformly random for \( \{\overline{Z}_i^{v_i}\}_{i=1}^n \) and send the matrix of hashes.

4) Extract input wired-labels for P2’s circuit from OT; receive GC, input wired-labels and matrix.
   Extract P2’s input to equality test.

5) Define the following \( g() \) on input \( x \):
   - use the bits of \( x \) to select \( \{\overline{w}_i^{z_i}\} \)
   - run GC evaluation as P1 would to get \( v' \)
   - Define vector \( \overrightarrow{Z} \) that P1 would use in equality test
   - return 1 iff \( \overrightarrow{Z} = = \overrightarrow{Z}' \)

6) receive \( g(x) \) and give it to P2.

7) if \( g(x) = = 0 \) or P2 abort, send ”abort” to ideal functionality otherwise send ”continue”.

References