Special Topics in Cryptography:
Practical Secure 2-Party Computation

Prof: Mike Rosulek

What will we learn about?
Practical Secure 2-Party Computation (2PC)

Secure computation:

example 1: location-based mobile service
"show me nearby restaurants"
proximity query on big database

example 2: medical research
statistical analysis of medical records

Example 3: remote diagnostic
security company: intrusion detection
run diagnostic test on server logs

Common: data necessary: held by several parties
sensitive
incentive to using this data collectively

goal: perform computation
learn nothing more than prescribed output

Surprising result: (1980s) using cryptography, can
solve problem of secure computation, for
ANY computation, via interactive protocol.

→ “feasibility” results only, not practical
This course: How do you make this practical?
- Focus on 2 parties
- Hot area of research, last 10 years

Note: "practical" ≠ "heuristic"
Still crypto research: formal, math models, proofs of security

How will we learn it?
- Dive in head-first to bleeding edge of research
- Goal: practice in: reading, writing, presenting
- Collectively produce a resource that’s useful to community

Part 1 of class:
- Readings, attending lecture, some HWs, glossary entries

Part 2:
- Read/present papers
- Writing summaries
- Give feedback to peers

Work load

<table>
<thead>
<tr>
<th>Work load</th>
</tr>
</thead>
</table>

I | → | II

Time (t) | Quarter