<table>
<thead>
<tr>
<th>Admin:</th>
<th>Projects - presentations start Wed 4/12, evaluations by 5 Wed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Quiz</td>
</tr>
<tr>
<td></td>
<td>Pset 4</td>
</tr>
</tbody>
</table>

Exposure Notification
### MCT: explain

[https://youtube.com/watch?v=8QYM25jpilO or dsf6nwxaxaVo](https://youtube.com/watch?v=8QYM25jpilO or dsf6nwxaxaVo)

### Sensing

**TC 4TL - 6 ft., 15 min. (?)**

- video of robots
- EM phantoms

- orientation of phone
- distance
- water (bodies) in between
- xmit power & model of xmitr phone
- indoor/outdoor
- masks?
- walls
- broken up exposures 3x 5min?
- can hear up to 30M away?

### Record:

- time
- power (RSSI)
- Orientation
- Location

Apple/Google collaboration GAEN
Google/Apple exposure notification
What to transmit?

- time-varying "chirp"
  (RPI - rolling proximity identifier)

  based on time & daily log
  (key mostly for compression)

  chirp = hash(key || time) (time to 15 mins)
(Draw figure on board)
Key Sharing Among Servers

Download all possibly-relevant keys

Key Server

Verification Server

Upload Index's Keys & Authentication Token

Authentication Token

Check & Notification

OS

Ranging & Comm

Contact's Smartphone

Chirps

1

Test Result & Authentication Token

Index Case's Smartphone

Steps

1. Install and enable app
2. Use keys to broadcast chirps
3. Test; if positive, upload keys
4. Download keys, check chirps heard, possibly notify of exposure

App

App

Public Health Authority
When to upload?

When test positive!

✔ PCR tests

DIY (antigen) tests

symptoms

Authentication (Authorization)

Auth code from PHA or test administrator

to prevent spamming of DB

consent required to upload

What to upload?

test type?

day # since infected? (estimate)
When /what to download? How to estimate risk level?

- Periodically
- Use risk formula to determine risk level
  - wide-net
  - narrow net
- Notes: must re-generate chips for keys
- Can't reconstruct "social graph"
- Consent needed to take action if notified
Attacks:

- Tracking (Linking)
- Relay attacks (simultaneous)
- Replay attacks (later) (pickup RPM's from test site)
- Spam DB ⇒ false notifications
- PU knows who tested positive, but not by whom
Effectiveness:

- reduce $R_0$ (infected by contact)
- scales as $p^2$, where $p$ = fraction with app
- Christoph Fraser et al. estimate 400K lives saved in UK.
- PH frustrated by lack of data (due to privacy)
- may depend on advice given as to what to do if notified
- see Prof talk by HCG 4/25 Monday 6:35 guest lecture
Issues & extensions:

- fixed beacons & fixed QR codes
- record what you send, rather than what you hear
  (e.g., index upload what he heard)
- CO2 sensor?
  Indoor/outdoor sensor?
  Fitbit?
- Governance - who decides what?
  PH versus private corporations?
  LE access? (centralized schemes)
- integration with MCT?
- multiple jurisdictions?