**Randori**

**Privacy-Preserving Data Collection**

Boel Nelson

boeln@chalmers.se

---

1. **Why local differential privacy?**
   - Enforced client-side
   - Participant never sends sensitive data
   - Data breach ≠ privacy breach
   - Simplicity of Randomized Response

2. **Randomized Response (RR)**
   - 'Yes' Truth
   - Truth 'No'
   - Fun fact: Randomized response is differentially private, but predates the concept of differential privacy by 41 years (1965 vs 2006)

3. **Why is RR not being used?**
   - End-to-end privacy
   - Accuracy-privacy trade-off

---

**Perfect Privacy** (Release no data) - Perfect Accuracy (Release all data)

Where the magic happens!

Accuracy

Privacy

---

**What is Randori?**

Randori is a set of tools:

A) Poll generator tool
B) Simulation environment
C) Server and client for data collection

**Purpose**

Make differential privacy accessible

---

**A. Poll Generator Tool**

- Features
  - Follow-up questions
  - Calculates \( \epsilon \)
  - Analytical accuracy bounds

---

**B. Simulation Environment**

- Features
  - Empirical accuracy results
  - Custom input distributions

---

**C. Data Collection**

- Features
  - Platform independent
  - Handles side-channels