

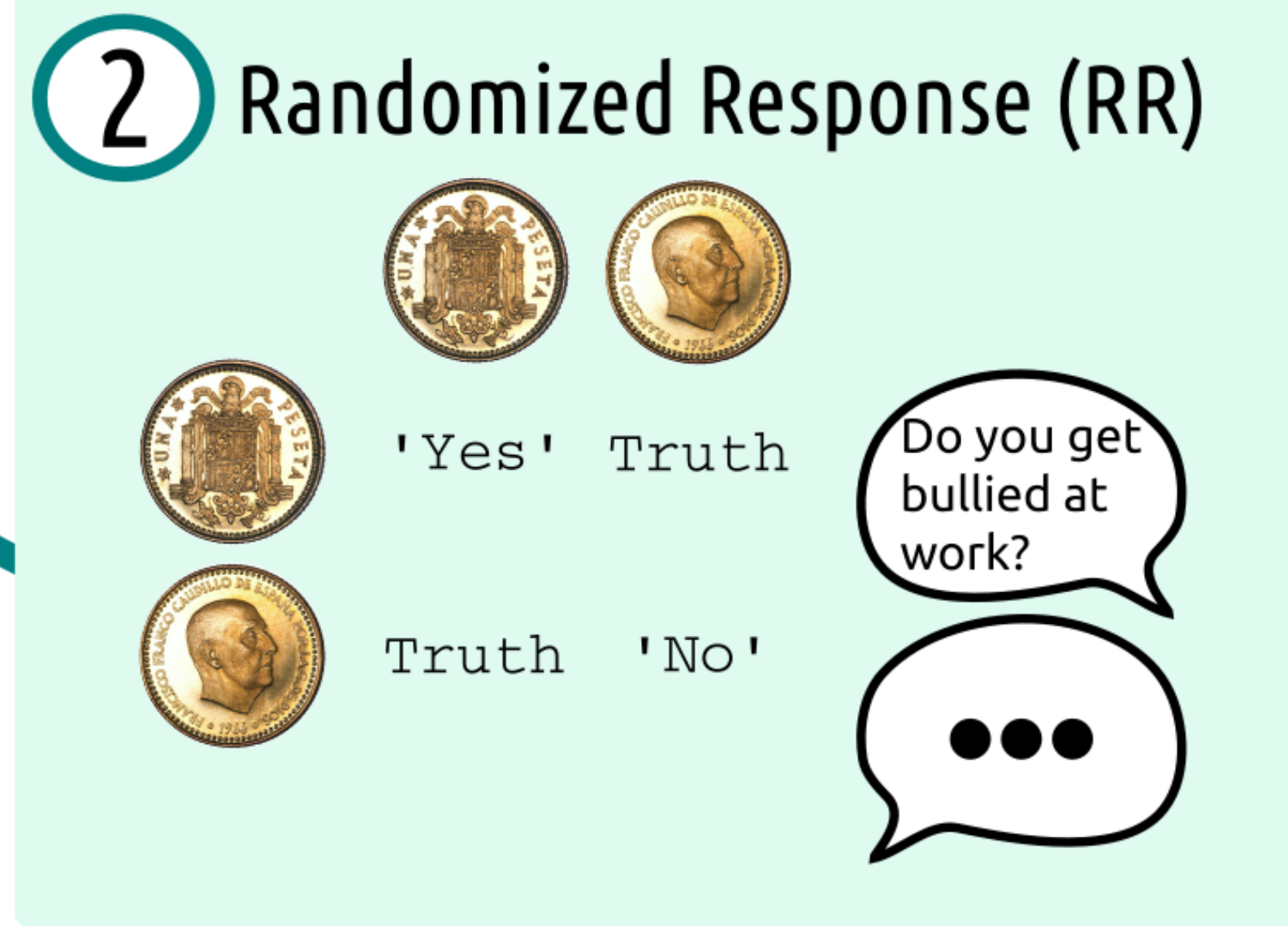
Randori

Privacy-Preserving Data Collection

Boel Nelson
boeln@chalmers.se

1 Why local differential privacy?

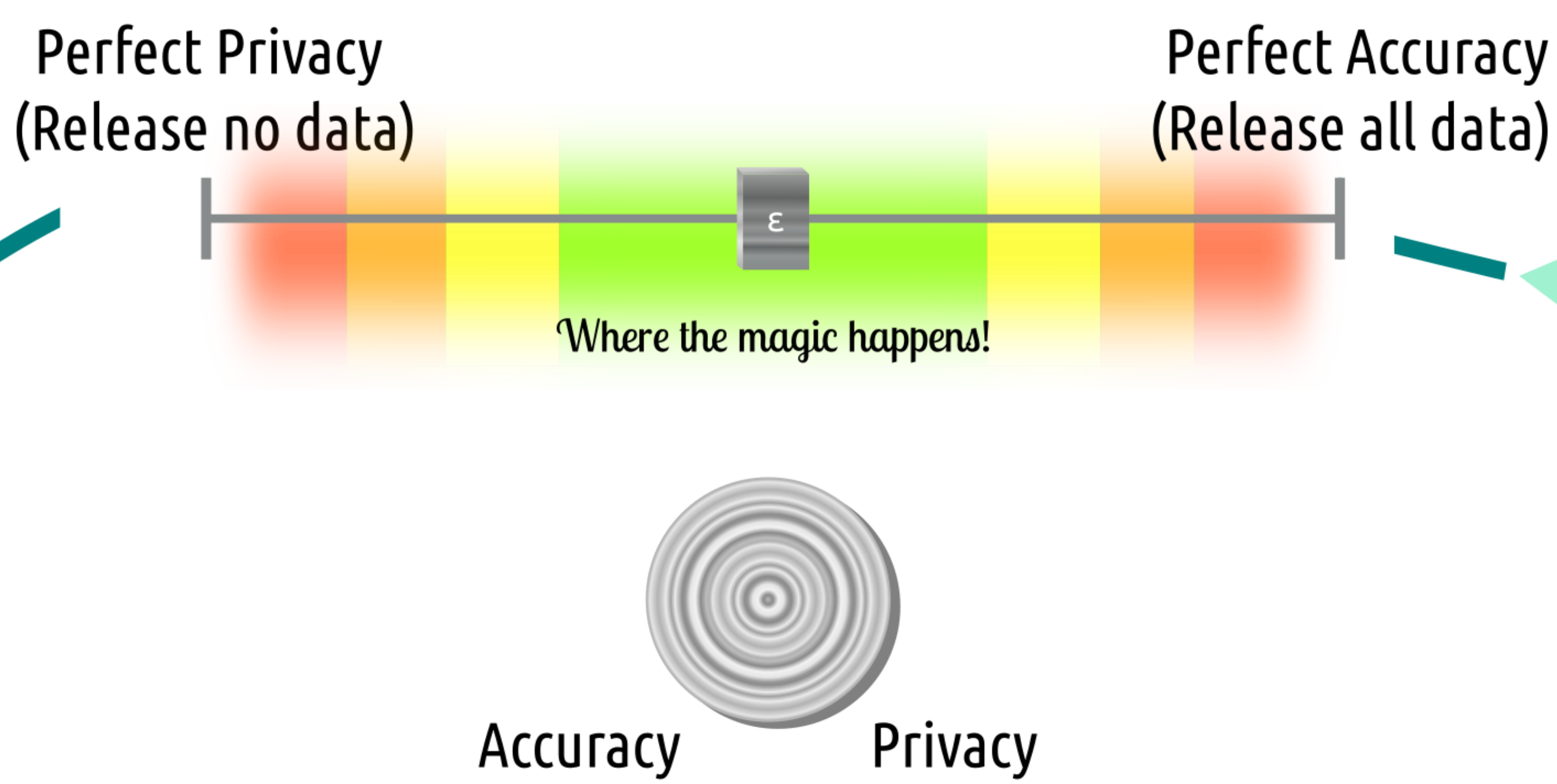
- ✓ Enforced client-side
- ✓ Participant never sends sensitive data
- ✓ Data breach \neq privacy breach
- ✓ Simplicity of *Randomized Response*



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



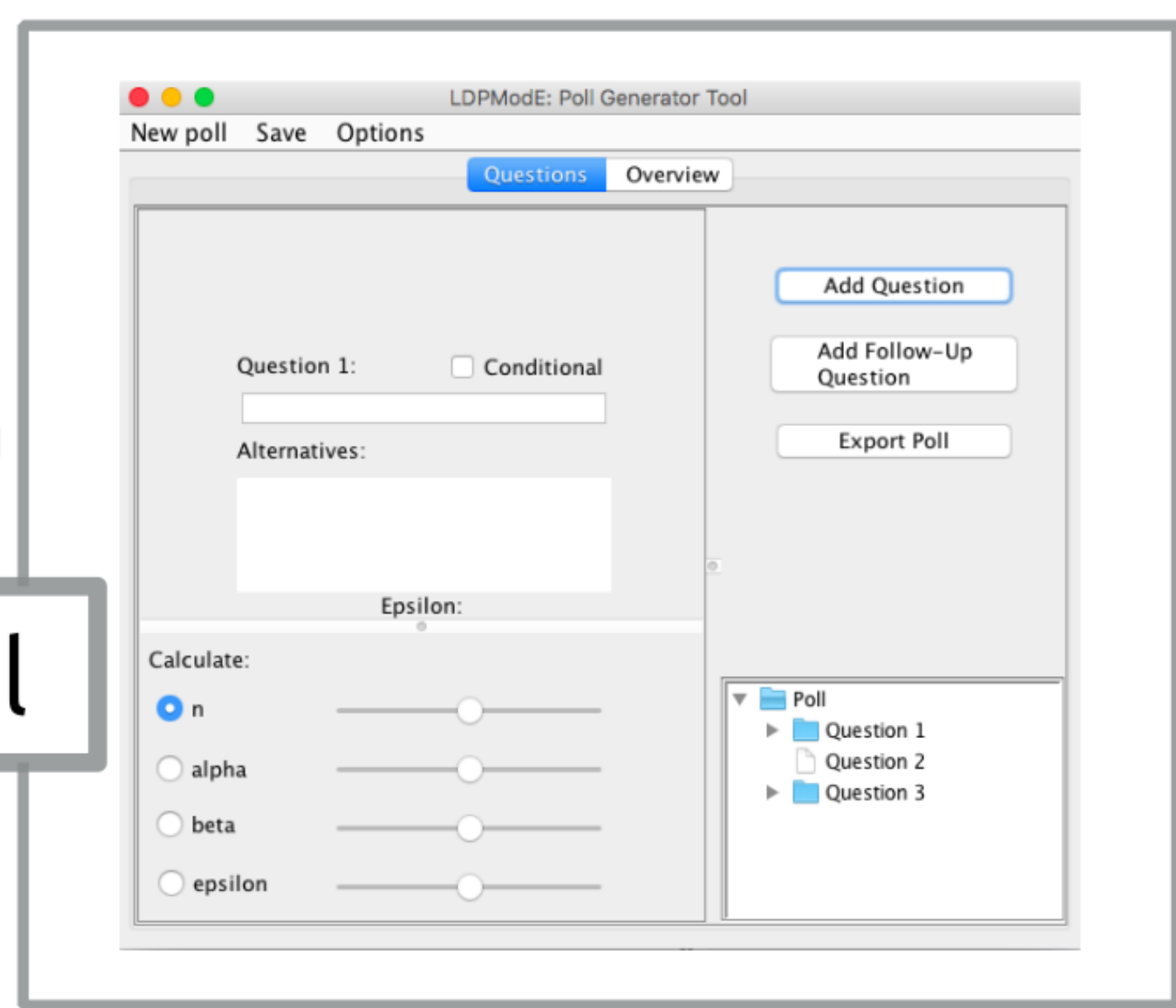
4 Privacy vs. accuracy

- > Trade-off
- > Empirical or analytical

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*

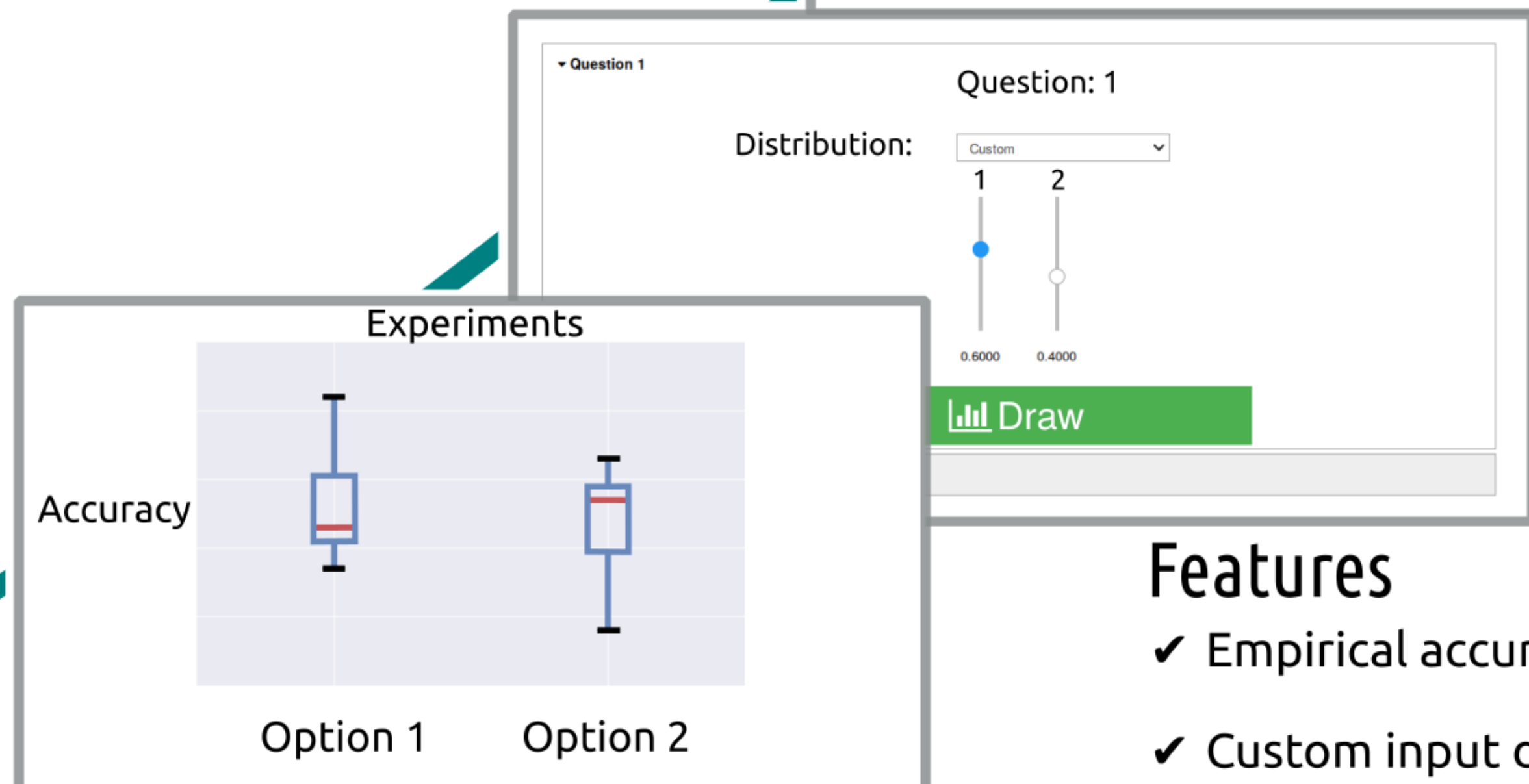
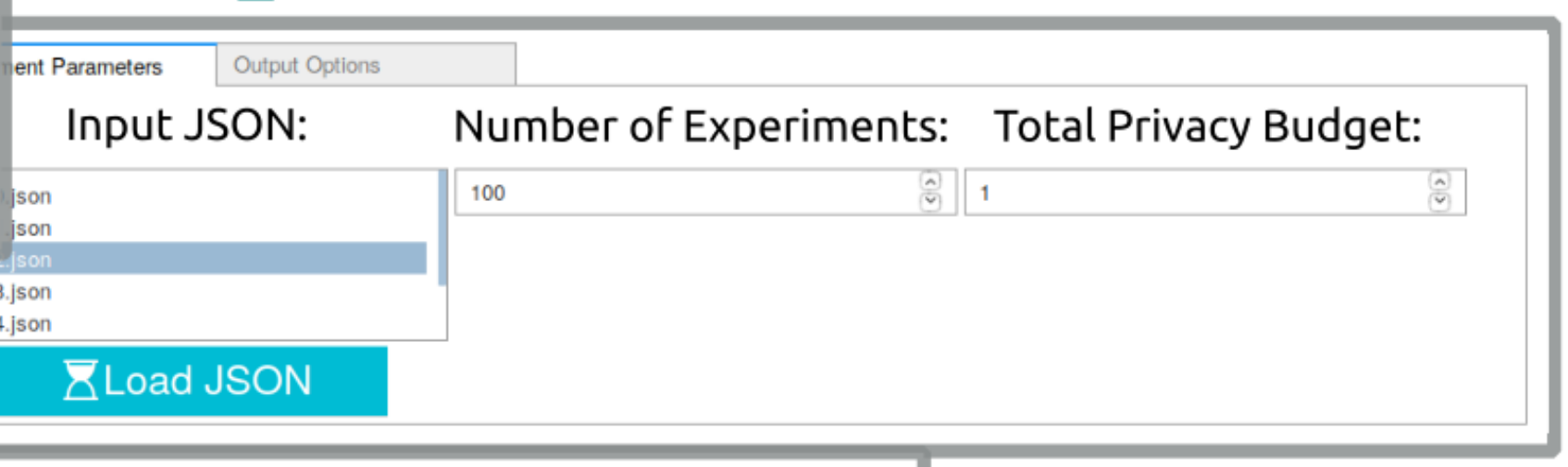


Features

- ✓ Follow-up questions
- ✓ Calculates ϵ
- ✓ Analytical accuracy bounds

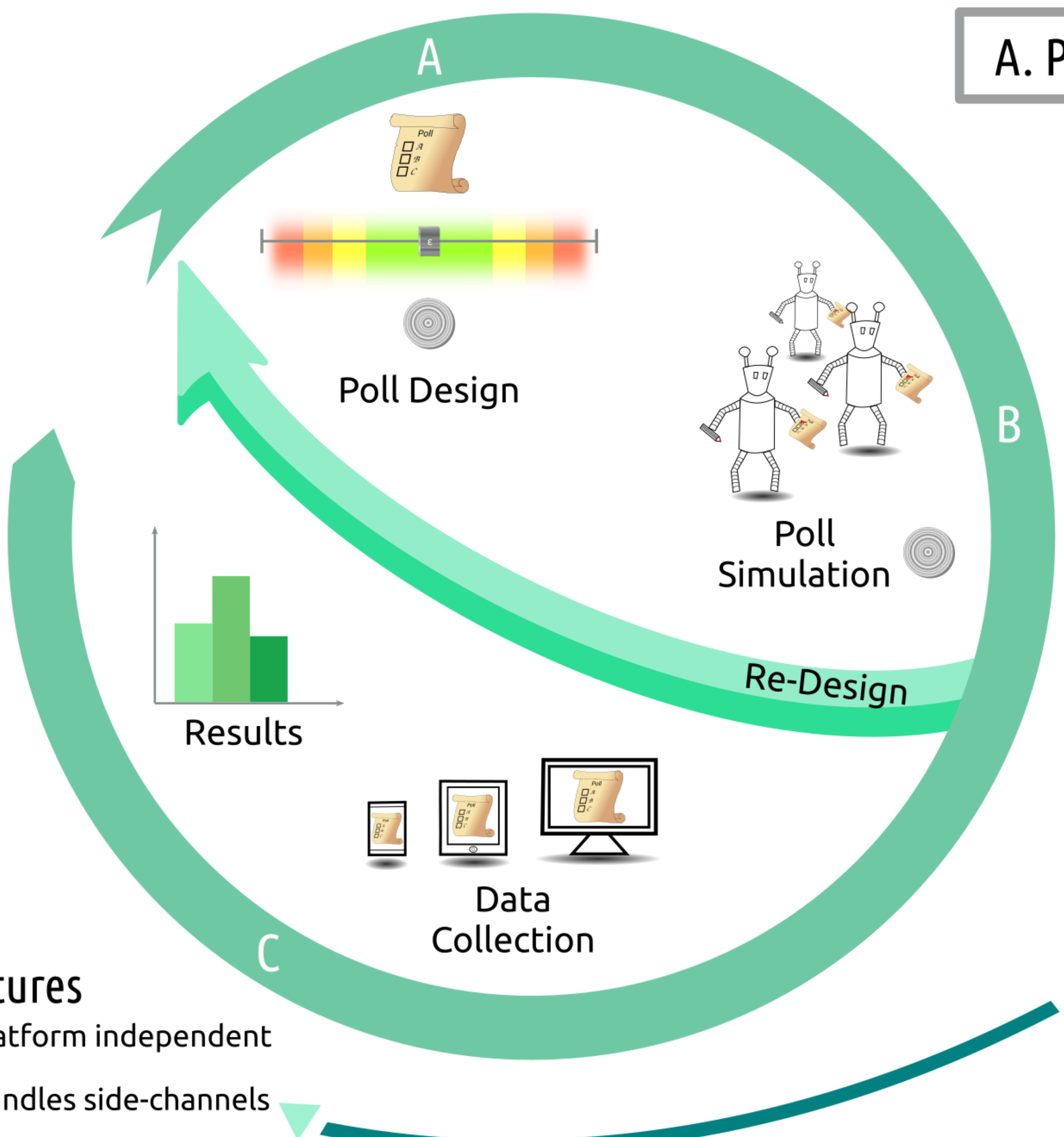
A. Poll Generator Tool

B. Simulation Environment



Features

- ✓ Empirical accuracy results
- ✓ Custom input distributions



Features

- ✓ Platform independent
- ✓ Handles side-channels