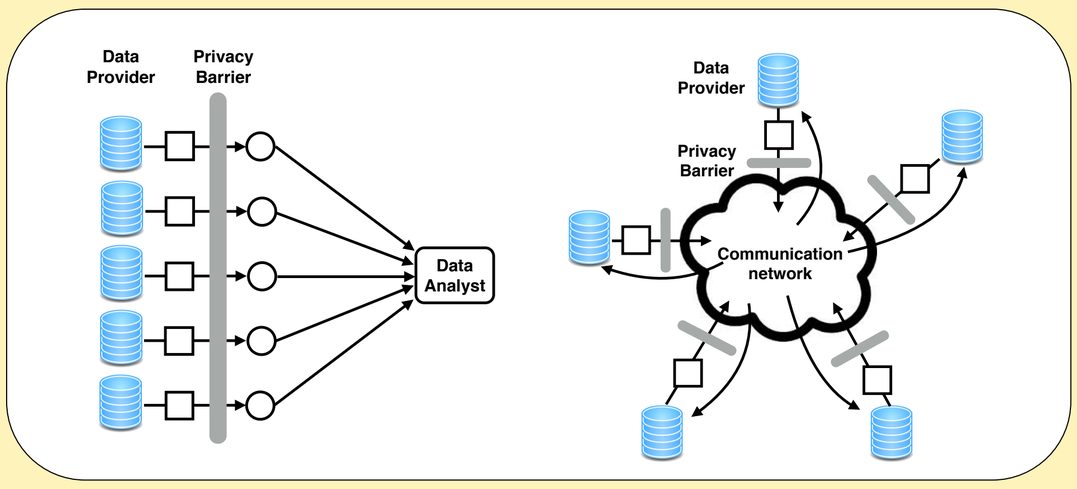
Fundamental limits in differential privacy

PI: Sewoong Oh, University of Illinois at Urbana-Champaign

The objective of this project is twofold.

Macroscopic analysis: To provide the mathematical foundations for macroscopic analyses of complex privacy-preserving systems, we will develop 'privacy calculus' which provides a new representation and corresponding computational tools for characterizing the fundamental limit on how those privacy guarantees operate.

Microscopic analysis: We will seek analytical characterizations (and numerical computational methods) for the fundamental tradeoff between privacy and utility under various canonical scenarios.



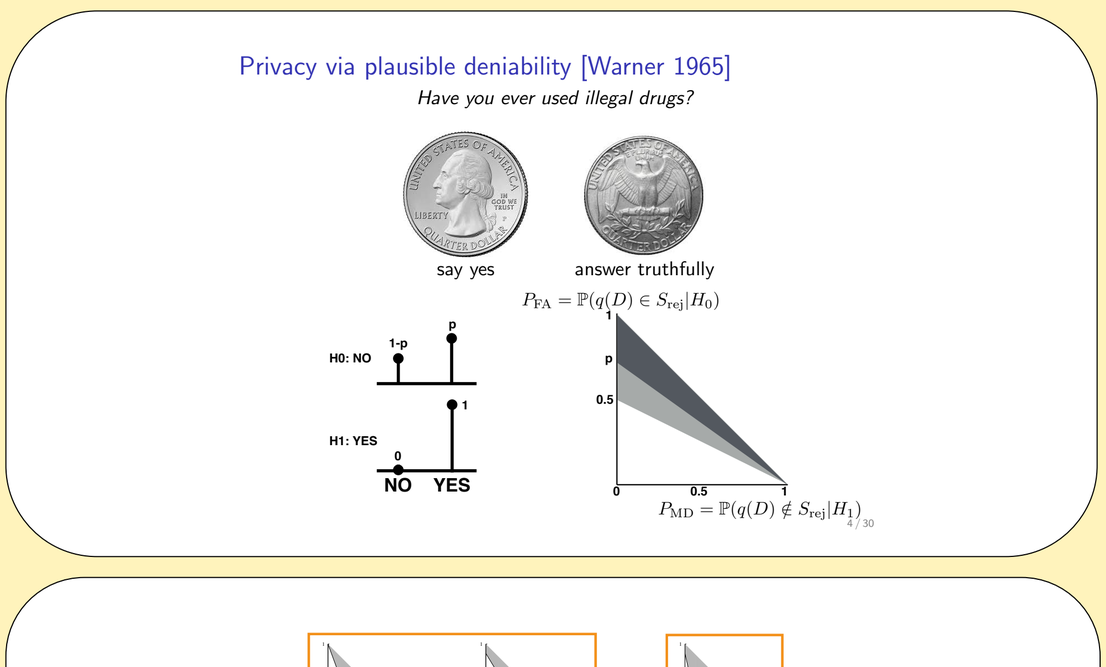
Approach

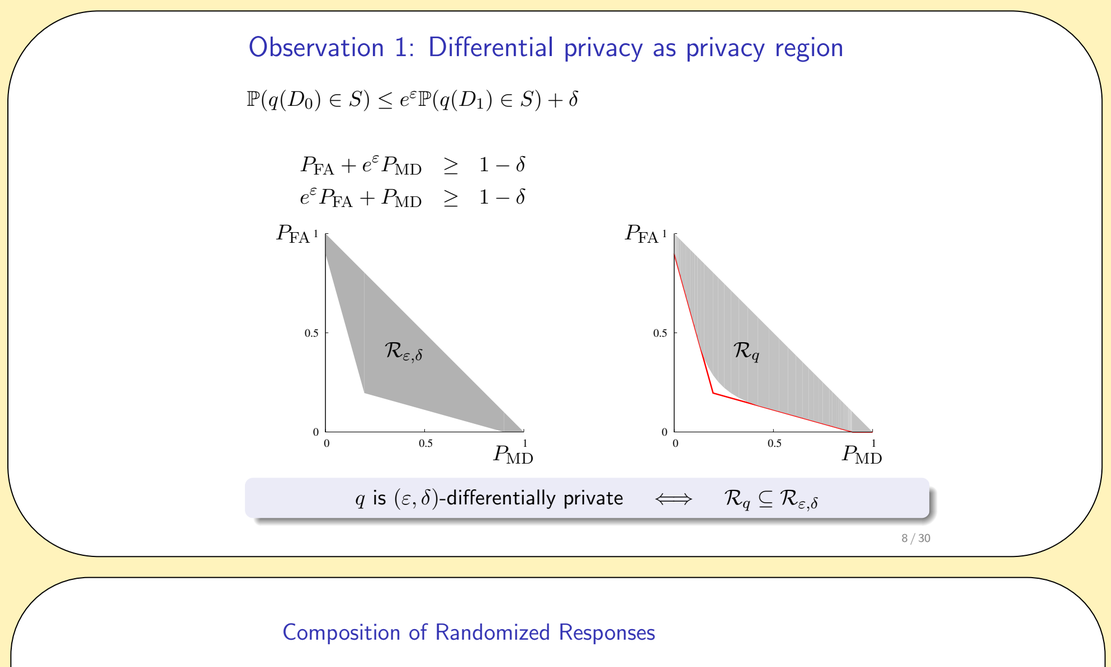
Privacy Region

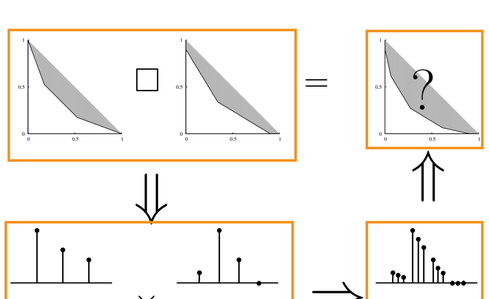
- Hypothesis testing interpretation of differential privacy provides a new representation using 2-D regions.
- This provides a foundation for privacy calculus for analyzing how privacy-preserving components interact

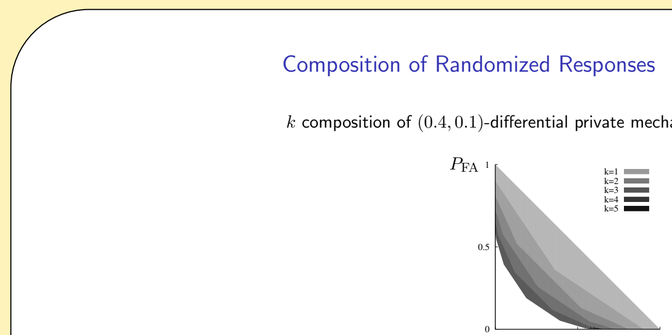
Staircase mechanisms

- The geometry of differential privacy constraints lead to a fanily of natural dominant mechanisms we call staircase mechanisms.
- This allows us to find the mechanism achieving optimal utility-privacy tradeoff









Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN