CS208: Applied Privacy for Data Science Conclusions

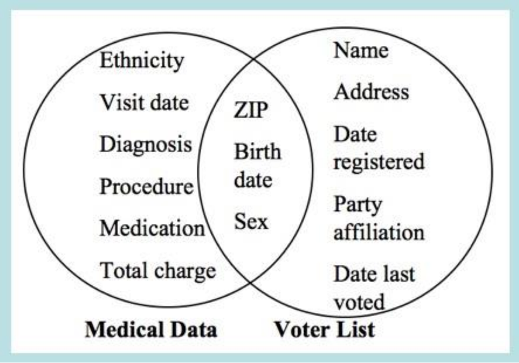
School of Engineering & Applied Sciences
Harvard University

April 26, 2022

Announcements

- My OH: tomorrow (Wed 4/27) 10:30-12:30 hybrid
- Final paper drafts due: Mon 5/2
- Poster session and class party: Mon 5/9, 2-5pm
  - Sign up for a presentation slot on Google sheet
  - If no one from your group can attend, we will schedule a separate time with you.
- Final paper revision: Fri 5/13
- Participation highlights II: Fri 5/13

Privacy Risks



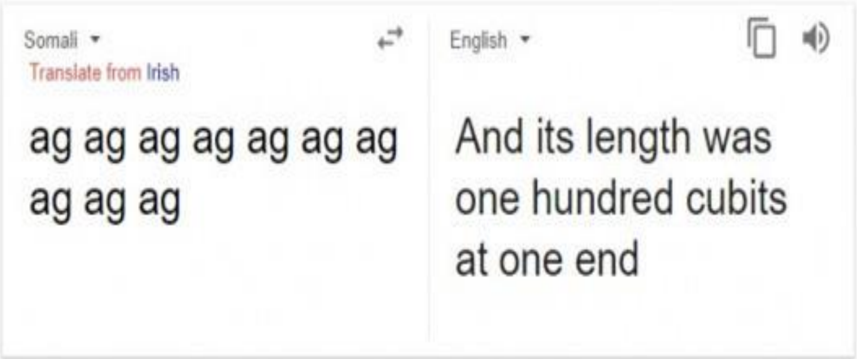
[Sweeney `97]

- Deidentified data can often be reidentified.

- Naïve query systems are subject to differencing-style attacks.

- Releasing too many aggregate statistics allows for reconstruction or membership attacks (Census, Diffix).

- Machine learning models can memorize their data and allow for membership attacks (Shokri et al., Google translate).



ag ag ag ag ag ag ag ag ag ag

And its length was one hundred cubits at one end

Definition of Differential Privacy

- Strong privacy definition.
- Compatible with many statistical analyses.
- Ensures that “individual-level information” does not leak.
- Applies regardless of adversary’s auxiliary information.
- Adversary can be external “analysts” (centralized DP) or aggregator (local DP) or in between (federated and shuffle).

But:

- Adversary may still infer sensitive attributes.
- Not applicable when utility requires individual-level data.
- “Privacy” has many other meanings beyond what is captured by DP.

Core Properties

DP is closed under post-processing:

“No adversary can break the privacy guarantee”

Group Privacy:

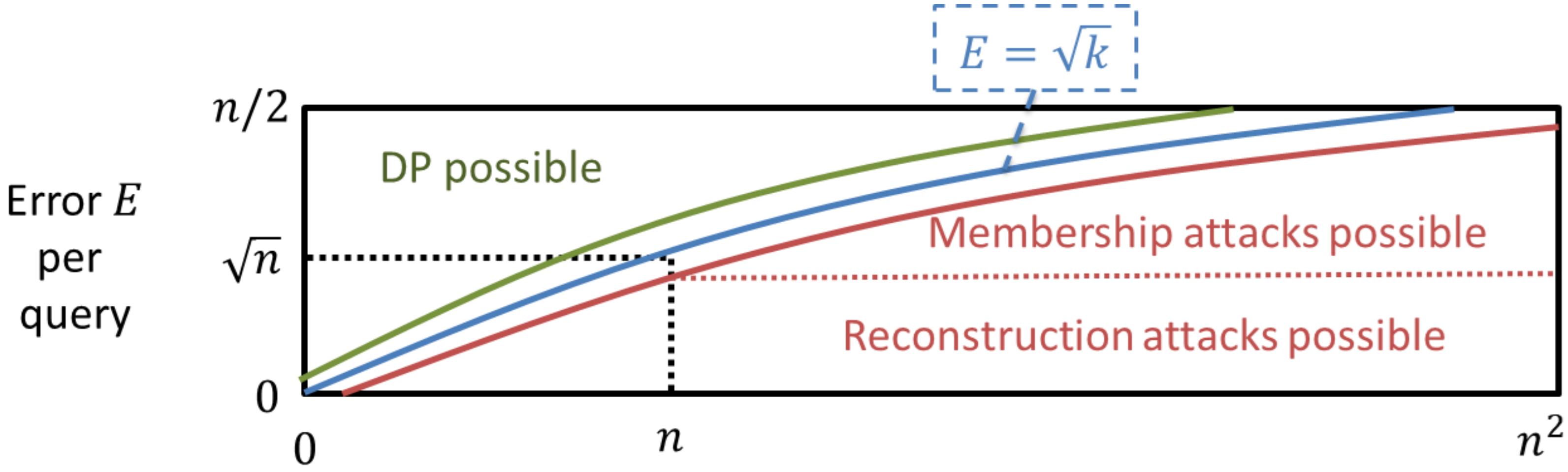
The level of privacy degrades linearly with the size k of the group

Differentially private mechanisms compose:

“The epsilons add up”

Composition of DP

- DP and variants (pure, approximate, zCDP, moments accountant) satisfy composition thms.
- Leads to tradeoff of # queries vs. accuracy (vs. privacy)



- Tradeoff is worse in local model.
- Allows for modular design of DP algorithms (w/post-processing).

Designing DP Algorithms

Any non-trivial DP mechanism must be randomized!

How to add noise and how much noise?

Scale to the query sensitivity (possibly after clipping)

- Means
- Medians/Quantiles/Ranges
- Histograms
- Regression (OLS & Logistic)
- Synthetic Data Generation
- Empirical Risk Minimization

- Deep Learning/DP-SGD
- Graph statistics
- Confidence intervals
- Causal inference (difference of means)
- Hypothesis tests

Core Components

A small number of primitives form the building blocks of some of the most complicated models, including:

- Clipping/Clamping
- Laplace and Gaussian Mechanisms
- Exponential Mechanism
- Randomized Response
- Composition
- Binning, One-hot encoding

As well as some core recurring ideas:

- Post-processing
- Lipschitz transformations
- Subsampling

More Building Blocks

Sparse Vector ($\Theta(\log k)$): we only care if the value of a query is important enough/above a certain threshold.

Offline correlated queries

- SmallDB: synthetic data generation

Online adaptive queries

- Private Multiplicative Weights (SparseVector!)

DP Programming Paradigms & Challenges

- Measurements, Transformations, Combinators (PINQ, OpenDP)
- Multi-relational databases (Flex, PrivateSQL, GoogleDP)
- User interfaces (DP Creator)
- General optimization/ERM/SGD (Opacus)
- Combining DP and other PETs (Private RCT)
- Formal verification of DP
- Finite-precision arithmetic
- Timing and other side-channel attacks

Experimental Investigation

Monte Carlo simulation methods are a valuable tool for investigating utility and other performance measures of algorithms. We have used this underlying template repeatedly:

1. Simulate data from distribution with known properties (or bootstrap from large dataset as if a population).
2. Release DP estimate and compare to true estimand.
3. Repeat 1 & 2 to integrate over simulation error and summarize.
4. Repeat 3 over free parameters of interest.

Value of Rigorous Thinking in Privacy & Security

- Break cycle of attack-defense-attack-defense-…
- Separates goal from solutions.
  - Can evaluate privacy/security definition on its own.
  - Opens design space for solutions.
- Makes assumptions about adversary and implementation explicit, evaluable.
- Allows for study of tradeoffs (e.g. privacy vs. utility) and limits (impossibility, hardness).

Societal Perspectives

- Contextual Integrity
- Taxonomy of Privacy
- Surveillance and modulation
- Bridging technical-legal gaps
- Essentially contested concept
- Social construction of technology vs. politics of technology
- Algorithmic formalism vs. realism
- Politics of DP

Deployments of DP

Census, Opportunity Atlas, Microsoft, Google, Apple, Uber, Meta, …

Challenges and Open Problems:

- Getting both sufficient utility and satisfactory privacy.
- Managing privacy budget over many queries and analysts.
- Compatibility with stakeholder practices & expectations
- Practical methods for generating synthetic data.
- Enabling analysts to interpret noise, perform inference, measure uncertainty.
- Social, political, ethical, legal considerations
- Side channel attacks (e.g. randomness, timing).
- Vetted and general-purpose software tools.
- Performing DP+MPC together efficiently

To Pursue Further at Harvard

- Some final projects may lead to publishable papers.

- Attend the Boston DP Summer School (6/6-6/10) and/or the Boston-area DP seminar

- Apply for an OpenDP/Privacy Tools internship.

- Explore annotated bibliography.

- Come discuss with us in office hours.

- Take Cynthia Dwork’s CS226r next year for more theory of DP and related topics (e.g. preventing overfitting, algorithmic fairness).

To Pursue Further Elsewhere

- Apply for a job as a privacy engineer/data scientist/researcher.
  - Big & small tech companies
  - Privacy start-ups
  - Government agencies
  - Privacy non-profits and advocacy organizations
  - Industries grappling with data privacy (healthcare, finance, …)
  - Follow OpenDP slack #jobs channel

- Apply to graduate programs at places doing DP (we're happy to provide advice).