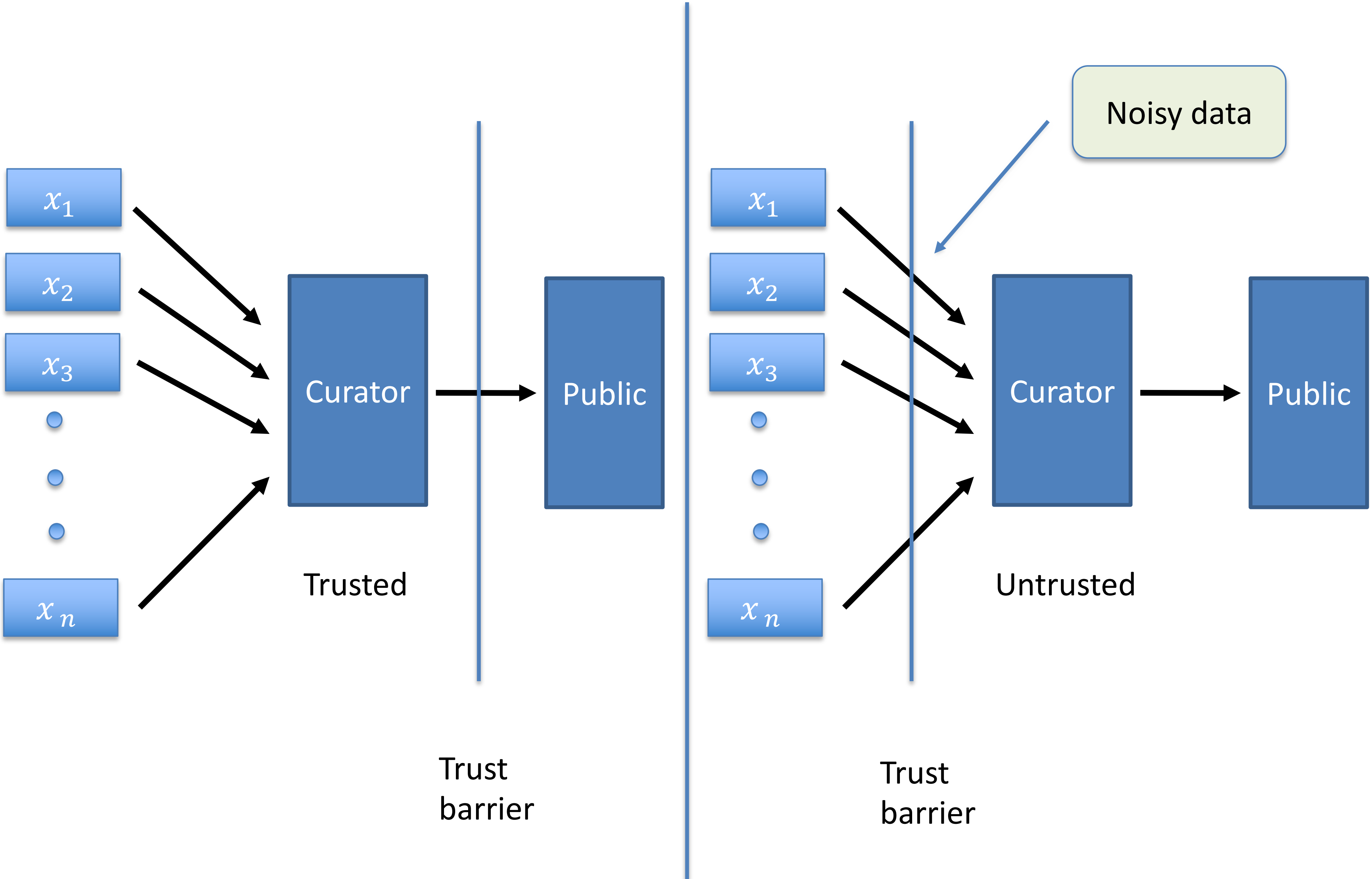
CS208: Applied Privacy for Data Science
The Local Model: Foundations

School of Engineering & Applied Sciences
Harvard University

March 28, 2022

Central Model vs Local Model



Central Model vs Local Model

- DP definition:

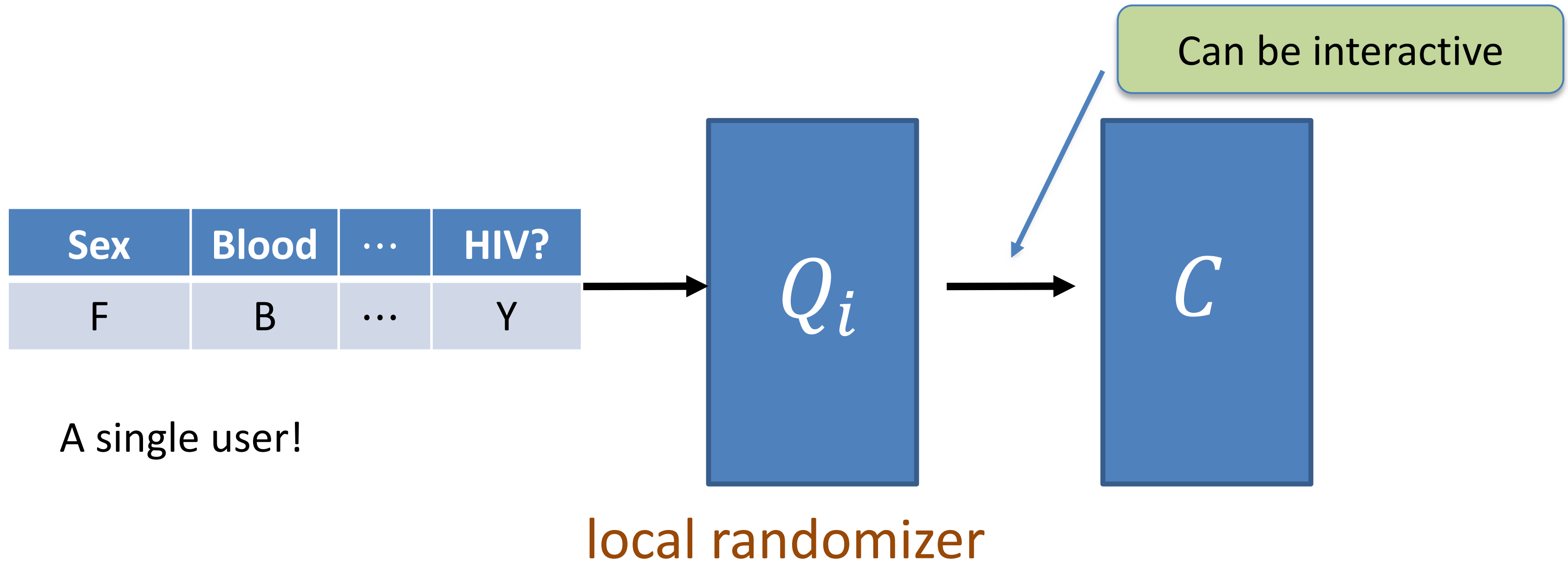
An algorithm $M: T^n \to R$ is $(\boldsymbol{\epsilon}, \boldsymbol{\delta})$**-differentially private** if $\forall$ neighboring $x, x' \in T^n$ and $\forall\, S \subseteq R$,

$$P[M(x) \in S] \leq e^{\epsilon}\, P[M(x') \in S] + \delta$$

- Only distinction: when the privacy perturbation needs to be applied!

- Leads to differences in what is meant by ``neighboring databases''

Local Differential Privacy



Local Randomizer $Q: X \to Y$ is $(\epsilon, \delta) -$ locally differentially private (LDP) if for all $x, x' \in X, S \in Y$

$$\Pr[Q(x) \in S] \leq e^{\varepsilon} \cdot \Pr[Q(x') \in S] + \delta$$

A protocol is ε-local DP if each party's local randomizer Q_i is an ε-DP mechanism for 1-row databases.

Randomized Response
[Warner'65]

- x_i: bits (binary)
- $y_i = \begin{cases} x_i & w.p.\ \frac{e^\epsilon}{1+e^\epsilon} \\ 1 - x_i & w.p.\ \frac{1}{1+e^\epsilon} \end{cases}$

Theorem: Each user's disclosure is ϵ-DP.

Mean Estimation by RR

- $\hat{\mu} = \frac{1}{n}\sum_i (\frac{e^{\epsilon}+1}{e^{\epsilon}-1} y_i - \frac{1}{e^{\epsilon}-1})$

- Unbiased estimator

- Accuracy $O\left(\frac{1}{\varepsilon\sqrt{n}}\right)$ (Chebyshev's inequality)

Randomized Response

ε-locally DP protocol that

- Estimates "statistical queries" (means/avgs) to $\pm O\left(\frac{1}{\varepsilon\sqrt{n}}\right)$.
  – Q: how to use RR for fractional-valued functions?
- Estimates count/sum of a bounded function to $\pm O\left(\frac{\sqrt{n}}{\varepsilon}\right)$.
  -- Q: proof idea?

- Worse than centralized DP, but still useful.

- This is best possible for ε-local DP.

Laplace Mechanism

Histograms

- $x_{1,} \ldots, x_n \in [D]$ (D bins)

x_i = | 0 0 0 … 1 0 … 0 …. 0 | Length D

Local Randomizer

y_i = | 1 -1 1 … 1 -1 … -1 …. 1 |

$$x_i = 0, \qquad y_i = \begin{cases} 1 & wp\ \frac{1}{2} \\ -1 & wp\ \frac{1}{2} \end{cases} \qquad\qquad x_i = 1, \qquad y_i = \begin{cases} 1 & wp\ \frac{1+\epsilon}{2} \\ -1 & wp\ \frac{1-\epsilon}{2} \end{cases}$$

$$\hat{f}(x) = \left(\sum_i y_i\right)\frac{1}{\epsilon}$$

Histograms

- Expected error on each bin is $\pm O\left(\frac{\sqrt{n}}{\varepsilon}\right)$.
- Expected max error over all D bins is $\pm O\left(\frac{\sqrt{n \cdot \log D}}{\varepsilon}\right)$.

- We need to communicate $\Omega(D)$ bits. There exists some sophisticated algorithmic ideas to get computational complexity sublinear in D.

Local vs. Centralized DP

Central Model

- Central curator collects the data from all users, then performs privatization
- Requires the users to trust the curator with their private data
- Most differentially private algorithms are in this model

Local Model

- Each user privatizes their own data then sends it to a central curator
- Require less trust from users
- Worse accuracy

Slide based on one from Brendan Avent's presentation

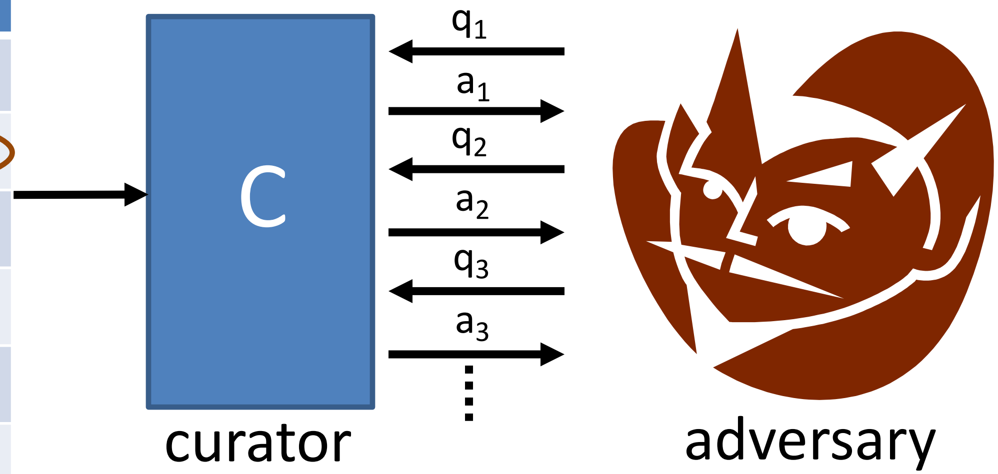
Defining Privacy

- Def: a protocol is ε-local DP if each party's local randomizer Q_i is an ε-DP interactive mechanism for 1-row databases.

- Q: What does it mean for an interactive mechanism to be DP?

DP for Interactive Mechanisms

Sex	Blood	⋯	HIV?
F	B	⋯	Y
F	A		Y
M	O	⋯	N
M	O	⋯	Y
F	A	⋯	N
M	B	⋯	Y



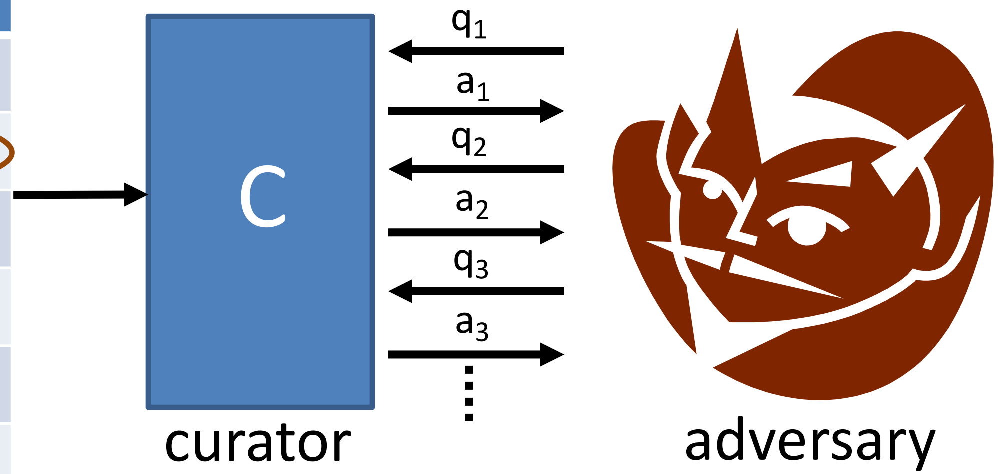
1st Attempt: for all D, D' differing on one row, all $q_1,\ldots,q_t$, all T

$$\Pr[C(D, q_1, \ldots, q_t) \in T] \leq e^{\varepsilon} \cdot \Pr[C(D', q_1, \ldots, q_t) \in T] + \delta$$

vectors of answers $a_1, \ldots, a_t$

DP for Interactive Mechanisms

Sex	Blood	⋯	HIV?
F	B	⋯	Y
F	A		Y
M	O	⋯	N
M	O	⋯	Y
F	A	⋯	N
M	B	⋯	Y



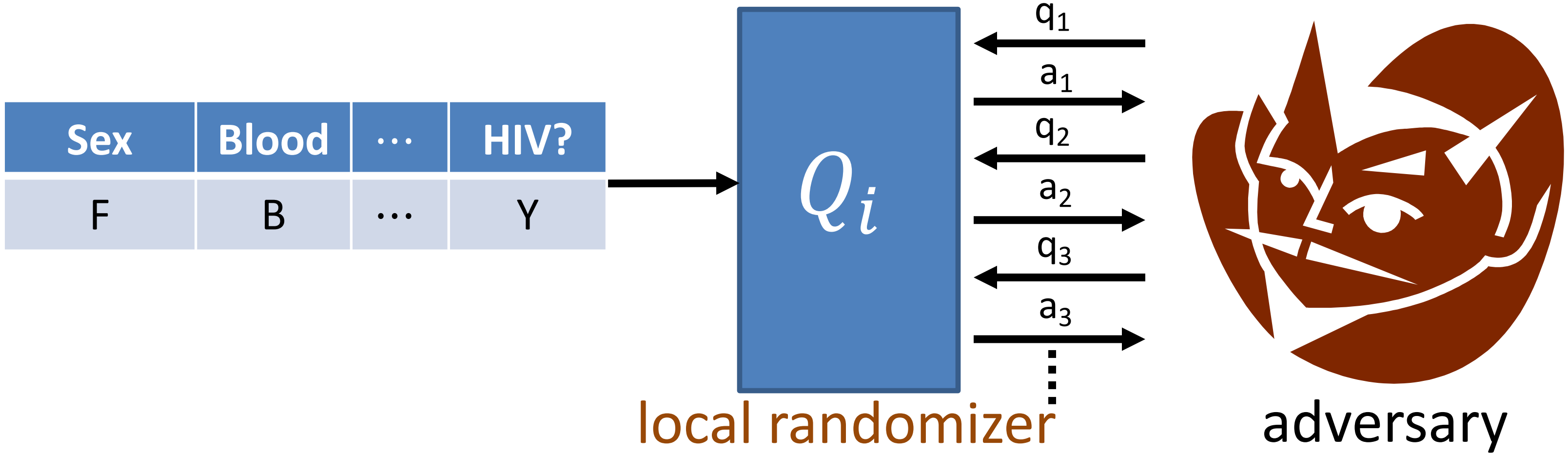
Better: for all D, D’ differing on one row, all adversarial strategies A

$$\Pr[A \text{ outputs YES after interacting w}/C(D)]$$
$$\leq e^{\varepsilon} \cdot \Pr[A \text{ outputs YES after interacting w}/C(D')] + \delta$$

Fact: composition thms for DP yield interactive DP in this sense.

(advanced/optimal comp. requires privacy params to be non-adaptive [Rogers et al. `16].)

Local DP



Require: for all i, x_i, x_i' ~~differing on one row,~~ all strategies A

$$\Pr[A \text{ outputs YES after interacting w}/Q_i(x_i)]$$
$$\leq e^{\varepsilon} \cdot \Pr[A \text{ outputs YES after interacting w}/Q_i(x_i')] + \delta$$

Local vs. Centralized DP

- Local DP protocols provably have lower accuracy for counts/averages than centralized DP protocols.
  - $\Theta(1/\varepsilon\sqrt{n})$ error vs. $\Theta(1/\varepsilon n)$.
  - Successful deployments have very large n (Google, Apple).

- Gap can be closed by relaxing adversarial model (e.g. anonymous participants, computationally bounded adversaries) and using crypto/infrastructure (secure MPC, mix-nets).