



# **CS208: Applied Privacy for Data Science**

## **The Local Model: Foundations**

School of Engineering & Applied Sciences  
Harvard University

April 1, 2022

# History of RR

Figure 1: An Example Warner Randomized Response Item

Please spin the following spinner in private and observe if it lands in section “A” or “B.” Do not tell me where it lands.

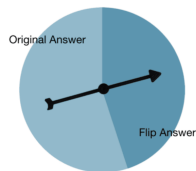
If the arrow landed in section “A,” respond True or False *only* with respect to statement A. If the arrow landed in section “B,” respond True or False *only* with respect to statement B.

**A:** I would be willing to pay a bribe to a police officer in order to avoid a traffic ticket. (True = I would be willing..., False = I would NOT be willing...)

**B:** I would NOT be willing to pay a bribe to a police officer in order to avoid a traffic ticket. (True = I would NOT be willing..., False = I would be willing...)

Please respond **TRUE** or **FALSE** now

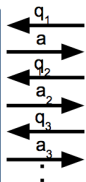
*Remember:* Your answers are completely confidential. Since only you know if the spinner landed in section A or B, no one else can know to which statement your answer corresponds.



See on NB: Gingerich 2015 “Randomized Response: Foundations and New Developments”

# Central Model

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

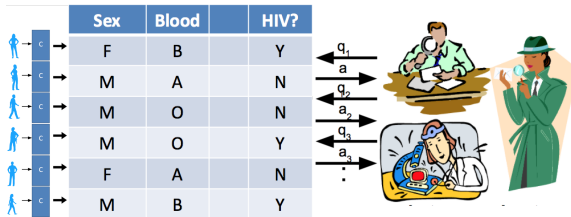


Data Repository

Curator

Analysts

# Local Model



Subjects      Repository

Analysts

## Example: Randomized response

- Each person has data  $x_i \in \mathcal{X}$ 
  - Analyst wants to know average of  $f: \mathcal{X} \rightarrow \{-1,1\}$  over  $x$
  - E.g. “what is the fraction of diabetics”?
- Randomization operator takes  $y \in \{-1,1\}$ :

$$Q(y) = \begin{cases} +y & w.p. \frac{e^\epsilon}{e^\epsilon + 1} \\ -y & w.p. \frac{1}{e^\epsilon + 1} \end{cases}$$

ratio is  $e^\epsilon$



- Observe:
  - If  $c_\epsilon = \frac{e^\epsilon + 1}{e^\epsilon - 1}$ , then  $E(c_\epsilon \cdot Q(y)) = y$
- How can we estimate a proportion?

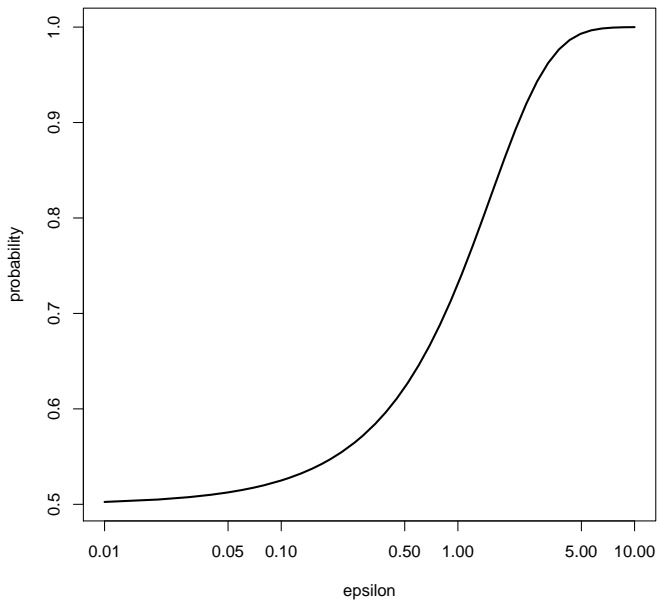
$$\text{➤ } A(x_1, \dots, x_n) = \frac{1}{n} \sum_i c_\epsilon \cdot Q(f(x_i))$$

- **Proposition:**  $E \left| A(x) - \frac{1}{n} \sum_i f(x_i) \right| \leq \frac{c_\epsilon}{2\sqrt{n}} \approx \frac{1}{\epsilon\sqrt{n}}.$

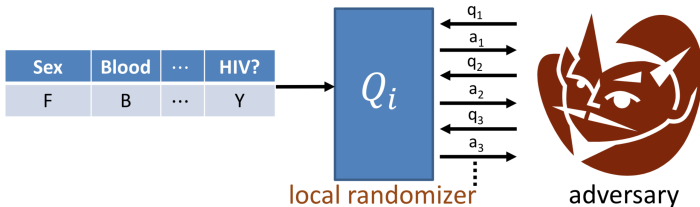
Contrast with  $\frac{1}{n\epsilon}$   
in central model  
(via Laplace noise)

Slide from Adam Smith

**Probability Truth Revealed in Local Model**



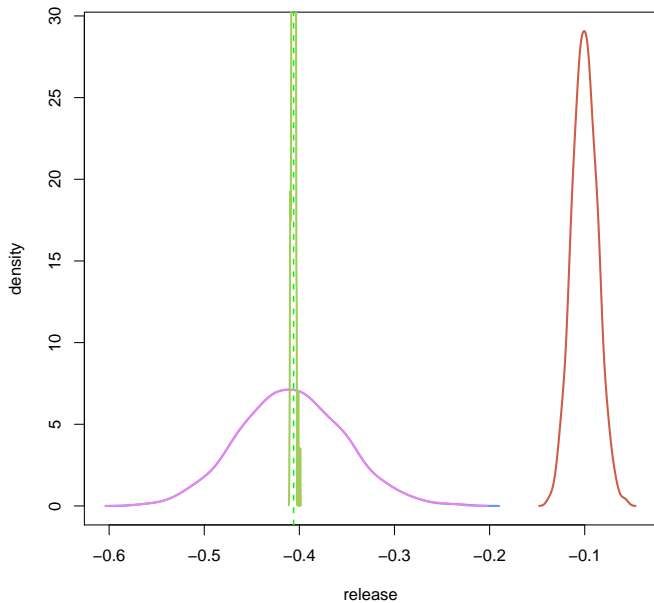
# Local DP



**Require:** for all  $i, x_i, x'_i$  ~~differing on one row~~, all strategies  $A$

$$\Pr[A \text{ outputs YES after interacting w/ } Q_i(x_i)]$$

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





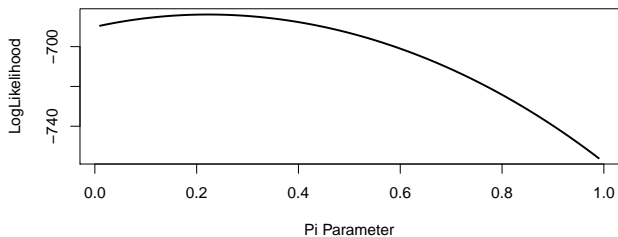
# Likelihood Based Correction

$$L(\theta|Y) \propto Pr(Y|\theta)$$

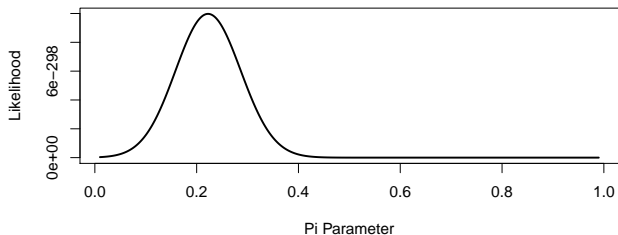
For  $Y \sim \text{Bernoulli}(\pi)$ :

$$L(\pi|Y) \propto \prod_{i=1}^N \pi^{y_i} (1 - \pi)^{1-y_i}$$

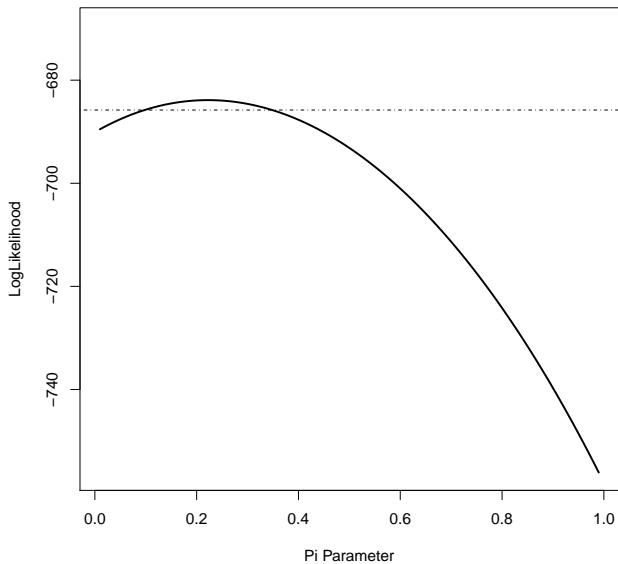
**LogLikelihood Surface**



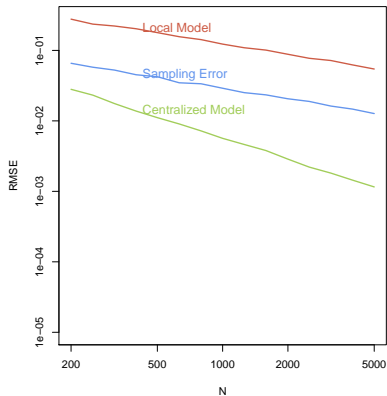
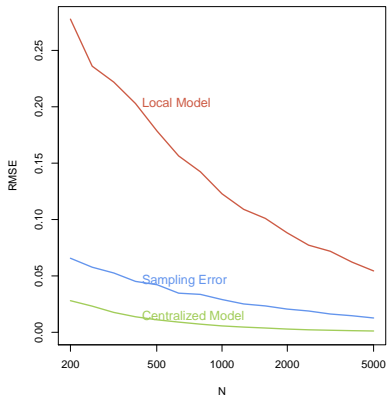
**Likelihood Surface**



**LogLikelihood Surface with Likelihood Ratio Test**

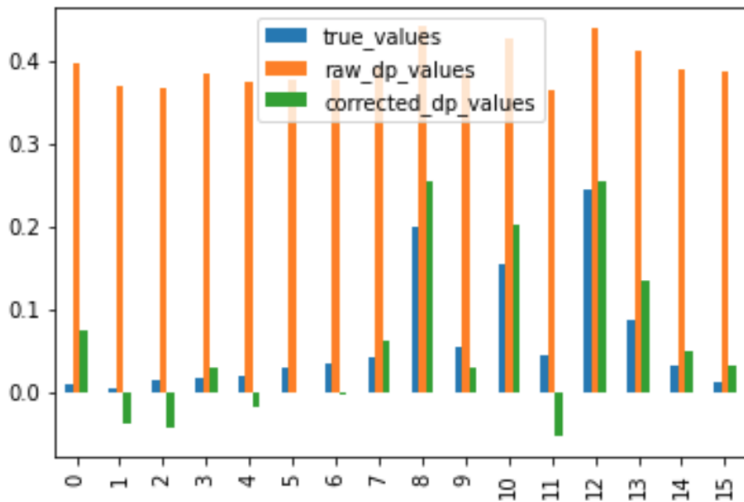


# Asymptotics of Error



$$\epsilon = 0.5$$

## Local Model for Integers/Histograms



$$\epsilon = 1, N = 2,000$$