Local Differential Privacy

Peter Kairouz

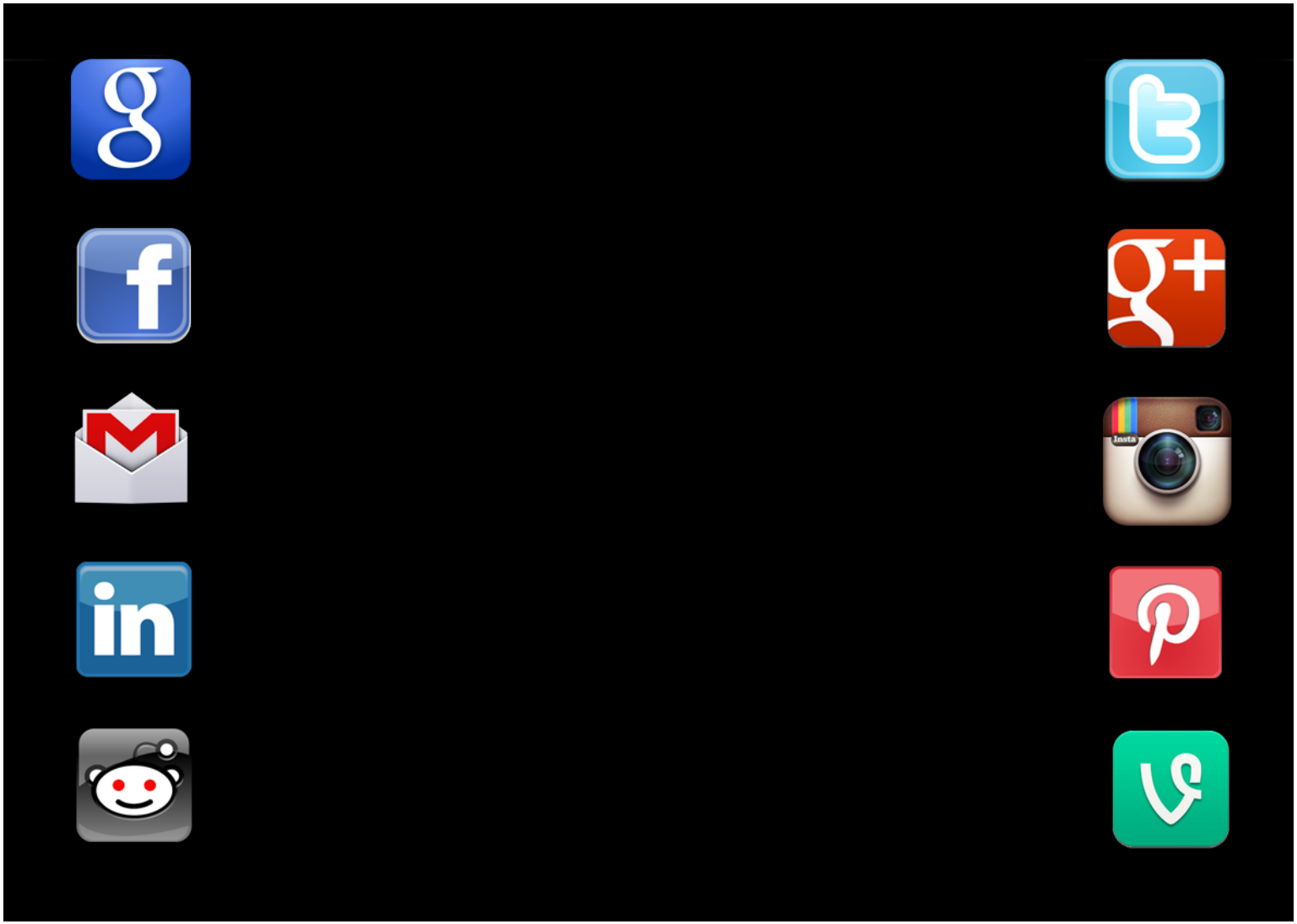
Department of Electrical & Computer Engineering
University of Illinois at Urbana-Champaign

Joint work with Sewoong Oh (UIUC) and Pramod Viswanath (UIUC)

Wireless Communication

The fundamental limits of digital communication are well understood

Rise of the Planet of the Apps!



Rise of the Planet of the Apps!

Rise of the Planet of the Apps!

Rise of the Planet of the Apps!

we study the **fundamental** trade-off between **privacy** and **utility**

Does Privacy Matter? [Greenwald 2014]

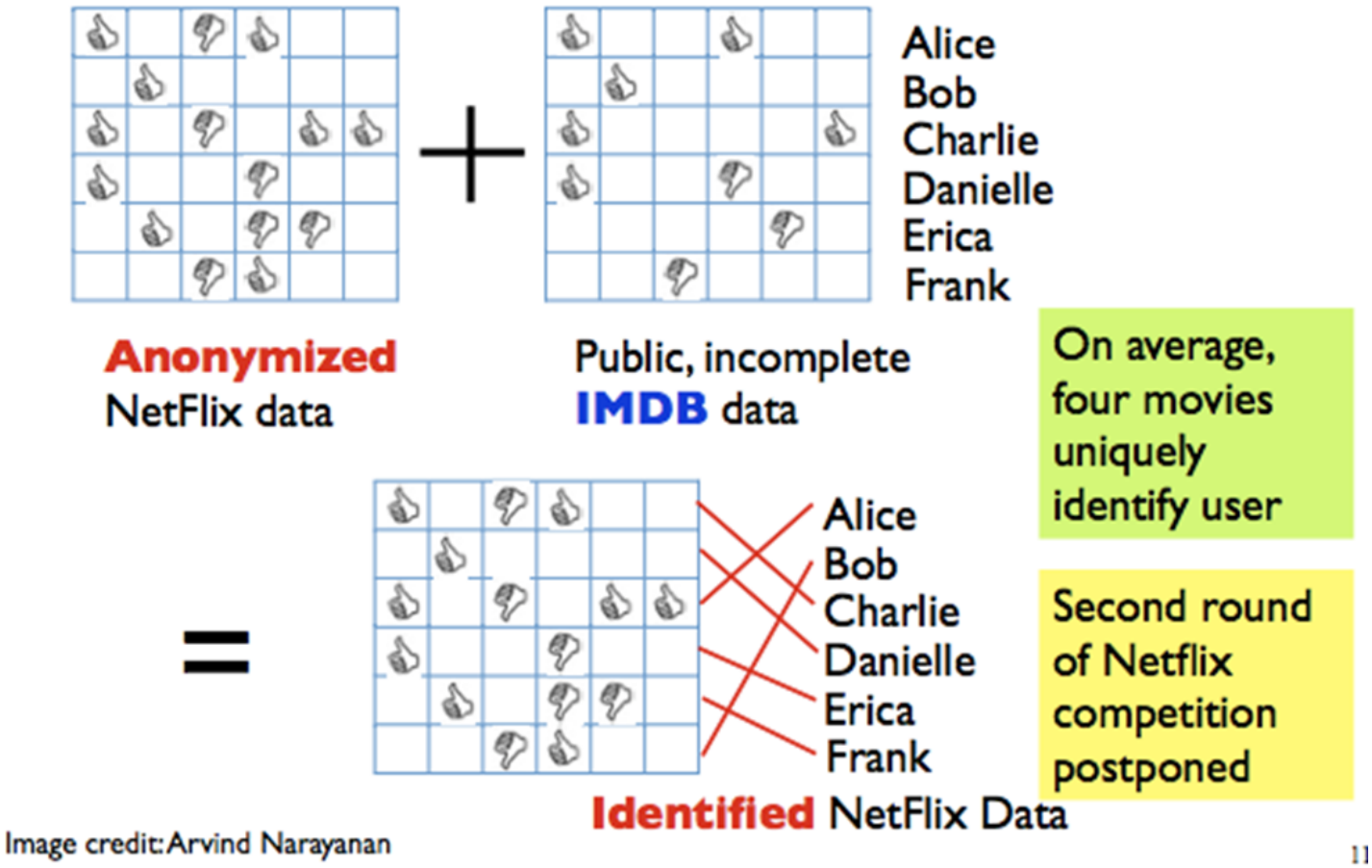
"If you're doing something that you don't want other people to know, maybe you shouldn't be doing it in first place"

"Privacy is no longer a social norm!"

Recent Privacy Leaks

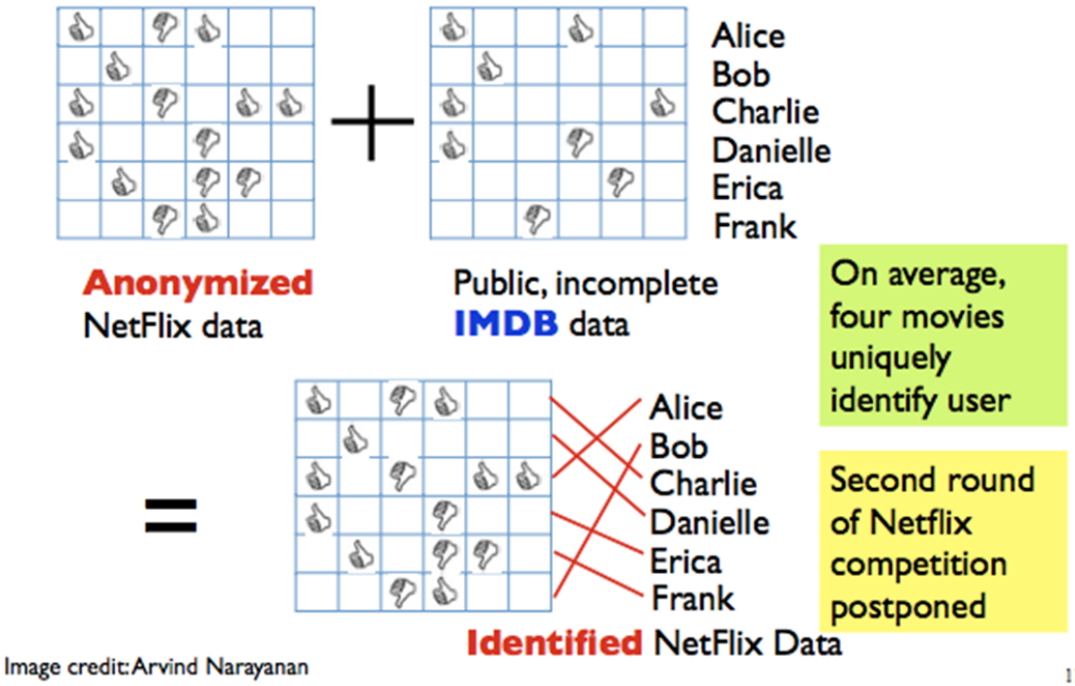
from **anonymous faces** to **social security numbers**

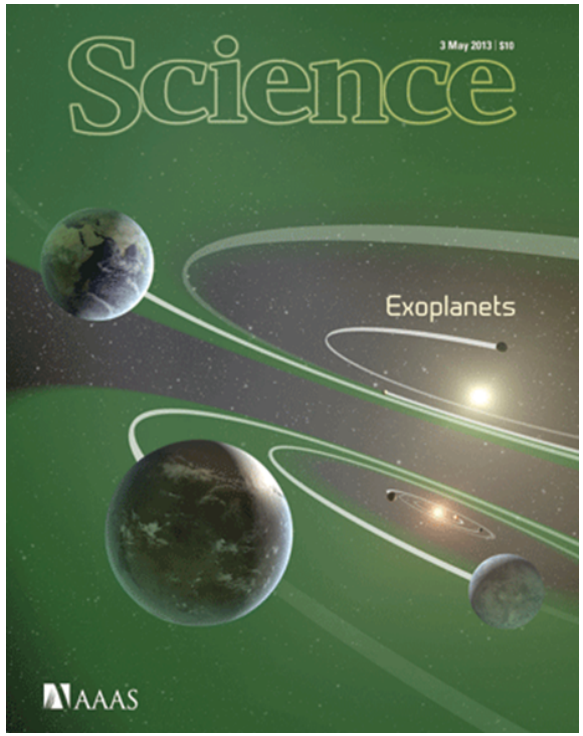
Recent Privacy Leaks



deanonymizing Netflix data

Recent Privacy Leaks





deanonymizing Netflix data, **identifying** personal genomes, etc.

Privacy is a **fundamental** human **right!**

The Ultimate Protection

"The future of privacy is **lying**"

randomizing = **systematic lying**

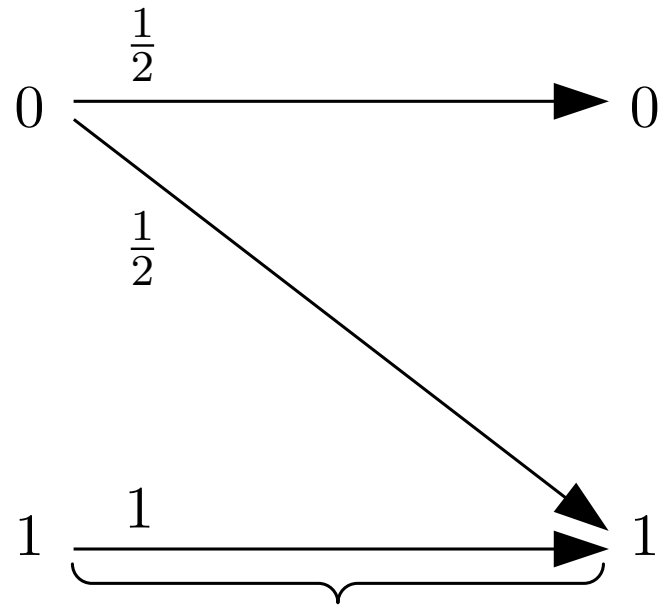
Privacy via Plausible Deniability [Warner 1965]

"Have you ever used illegal drugs?"

say **yes**

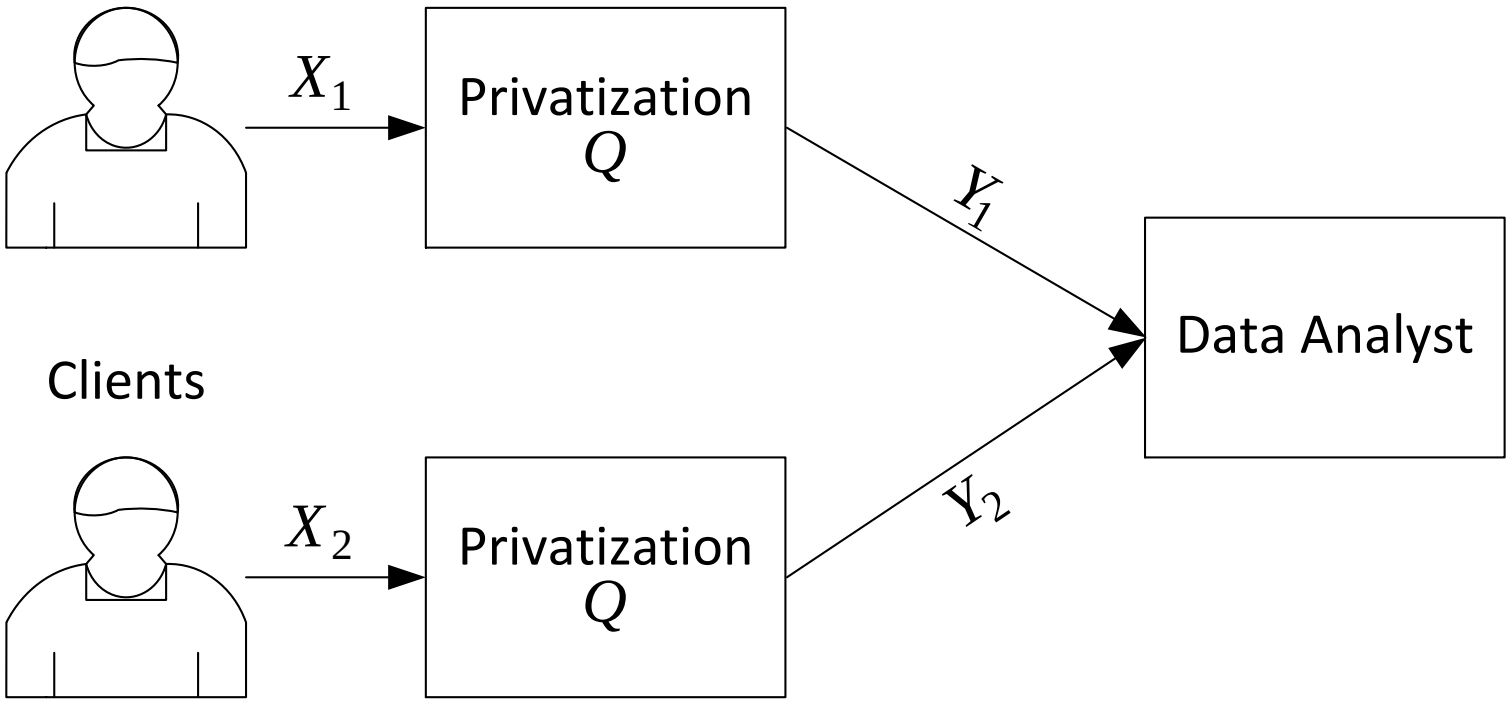
answer **truthfully**

Privacy via Plausible Deniability [Warner 1965]



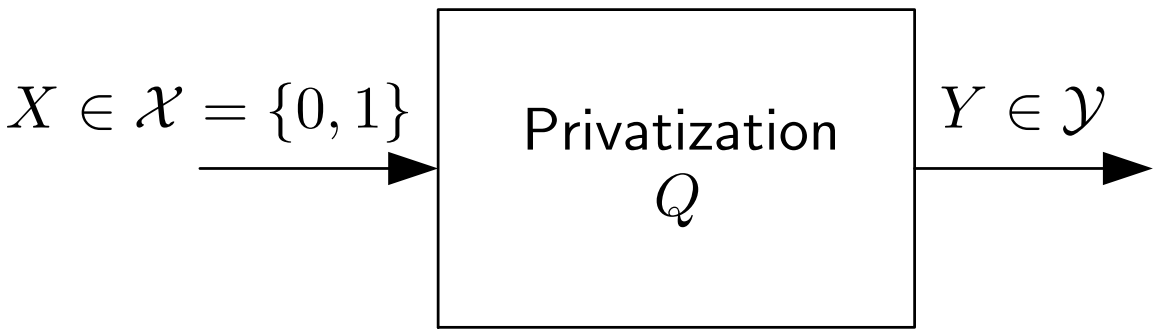
- instead of $X = x$, share $Y = y$ w.p. $Q(y|x)$
- $Q : |\mathcal{X}| \times |\mathcal{Y}|$ stochastic mapping

The Local Privacy Model [Duchi, et. al., 2012]



- clients **receive a service** if they share their data
- clients **do not trust** data analysts

Inference of Information

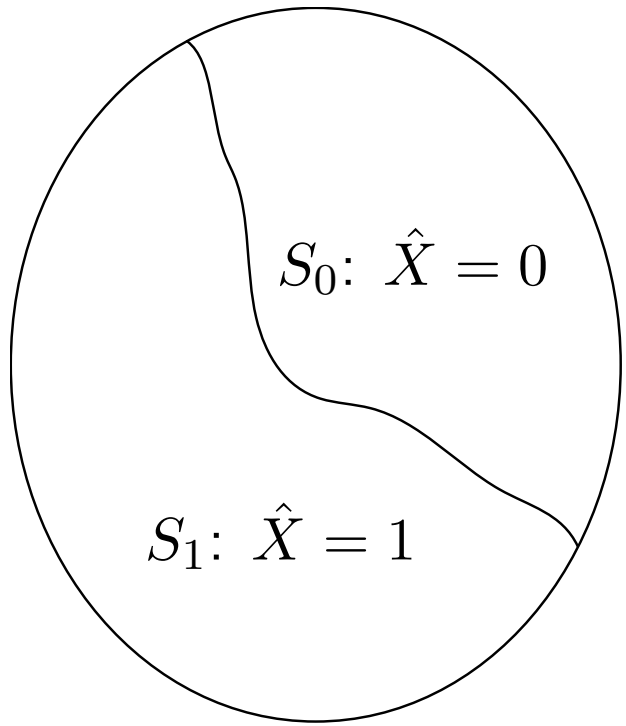


- $\mathcal{X}$: input alphabet
- $\mathcal{Y}$: output alphabet

Given $Y = y$ and Q, detect whether $X = 0$ or $X = 1$

Inference of Information

- given Y and Q, detect whether $X = 0$ or $X = 1$
- **two types of error**: **false alarm** and **missed detection**

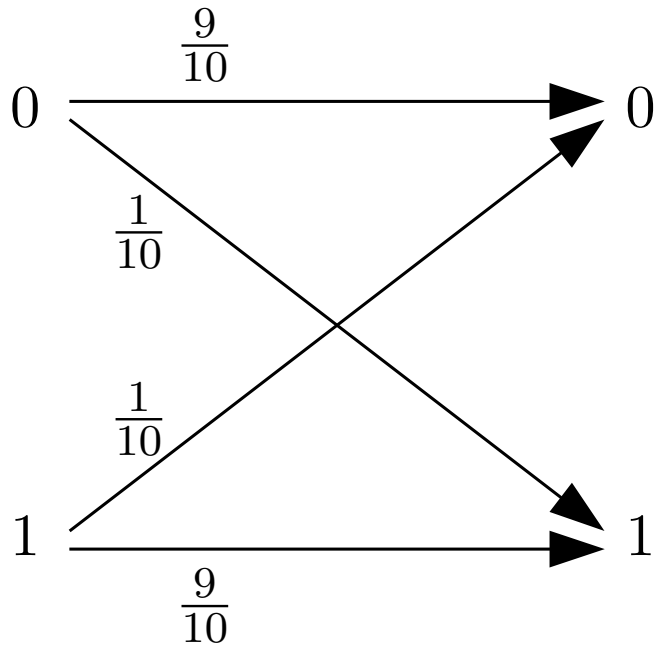


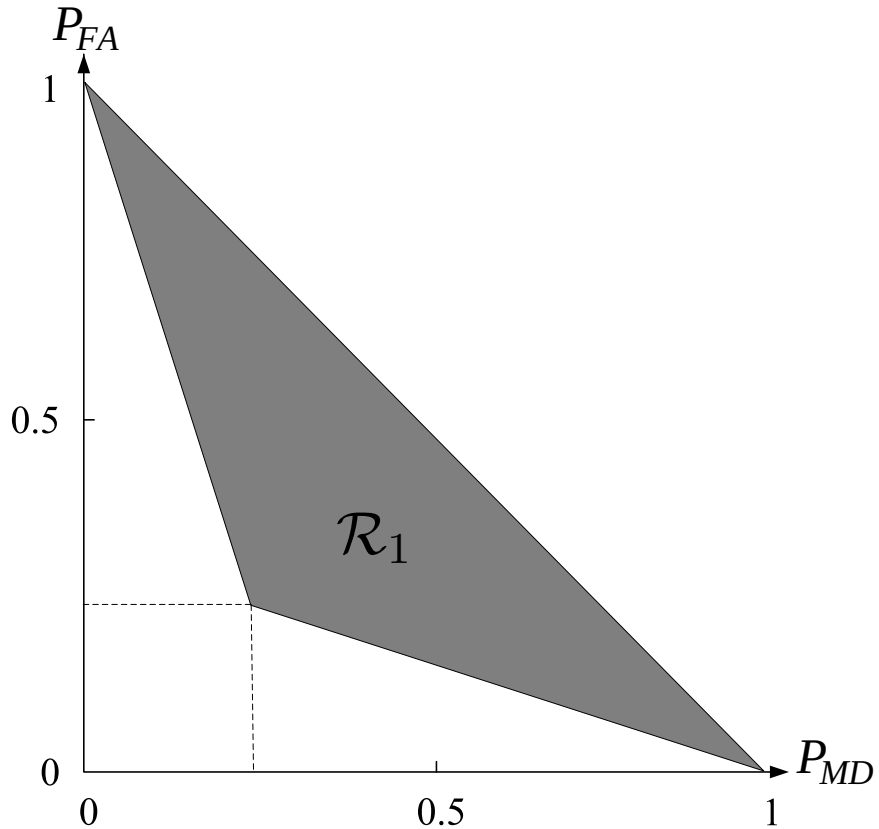
$\mathcal{Y}$: output alphabet

$P_{\mathrm{FA}} = \mathbb{P}(Y \in S_1 | X = 0)$ and $P_{\mathrm{MD}} = \mathbb{P}(Y \in S_0 | X = 1)$

Inference of Information

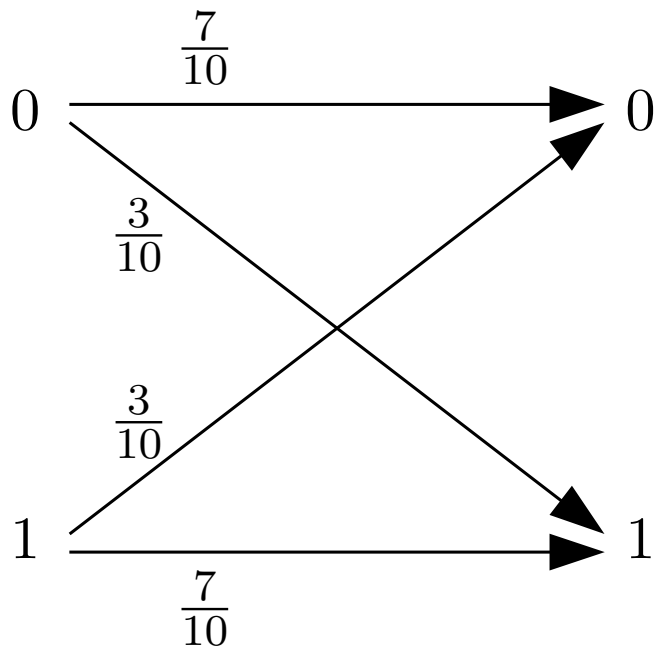
Case 1: Q_1

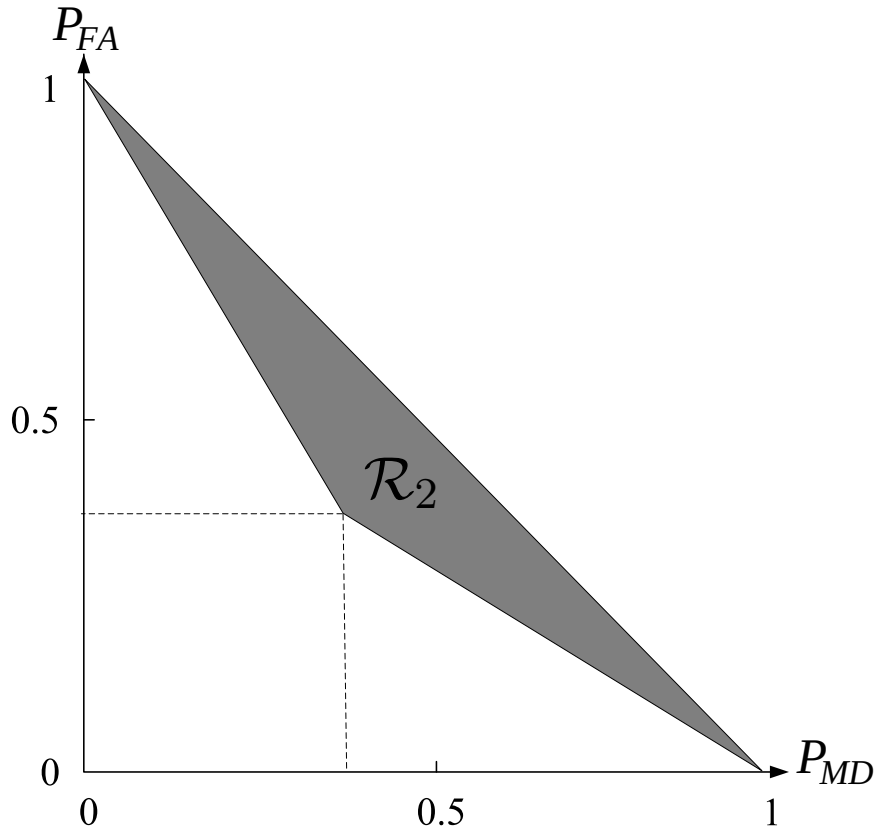




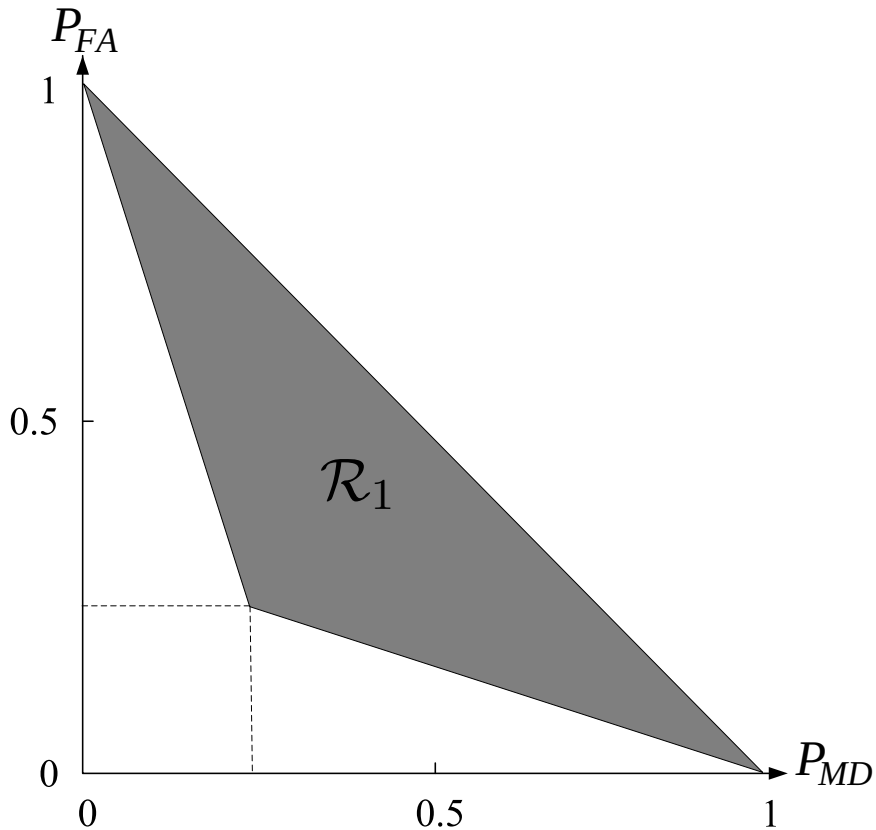
Inference of Information

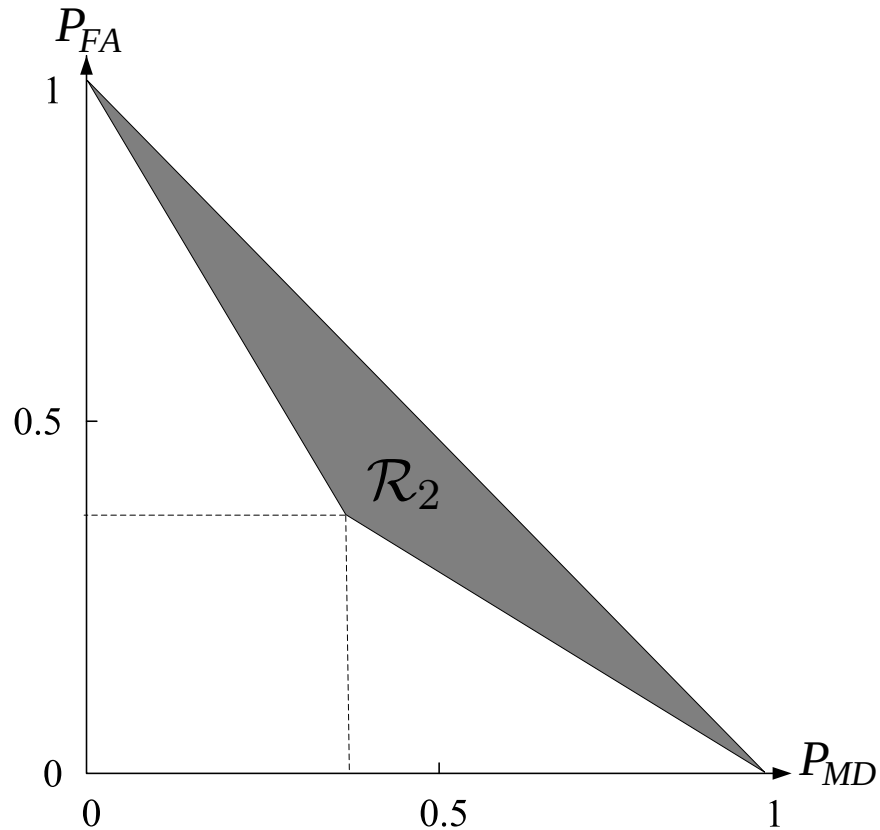
Case 2: Q_2





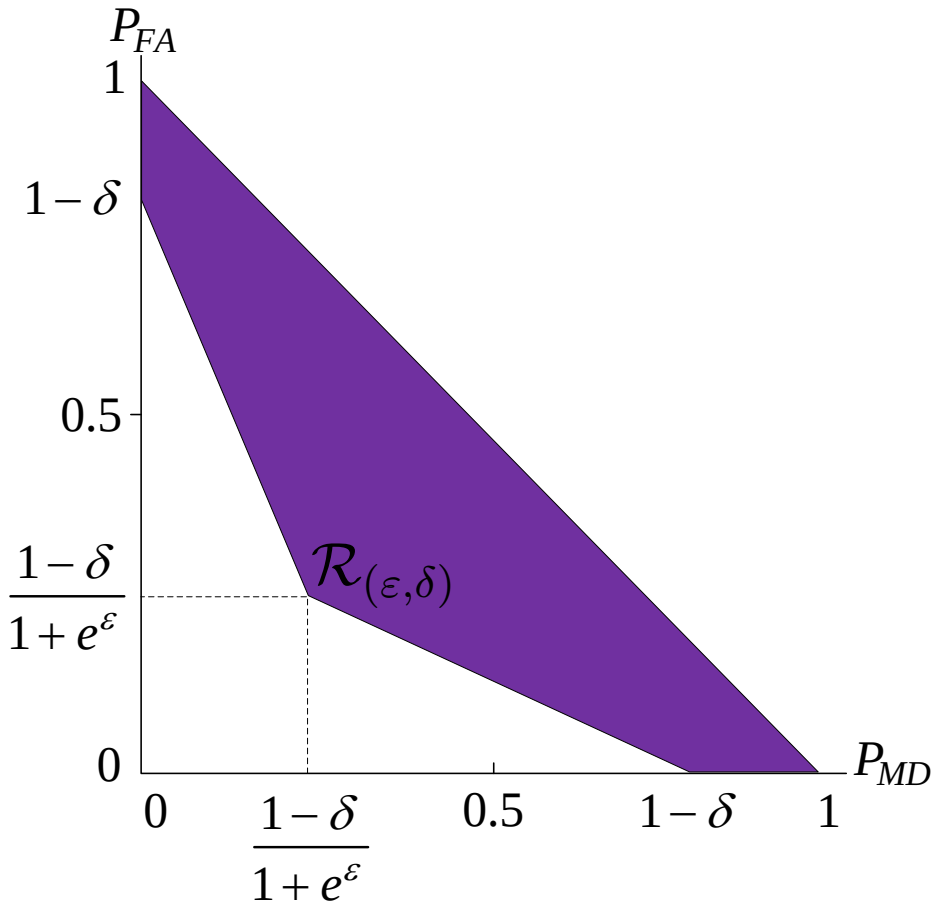
Inference of Information



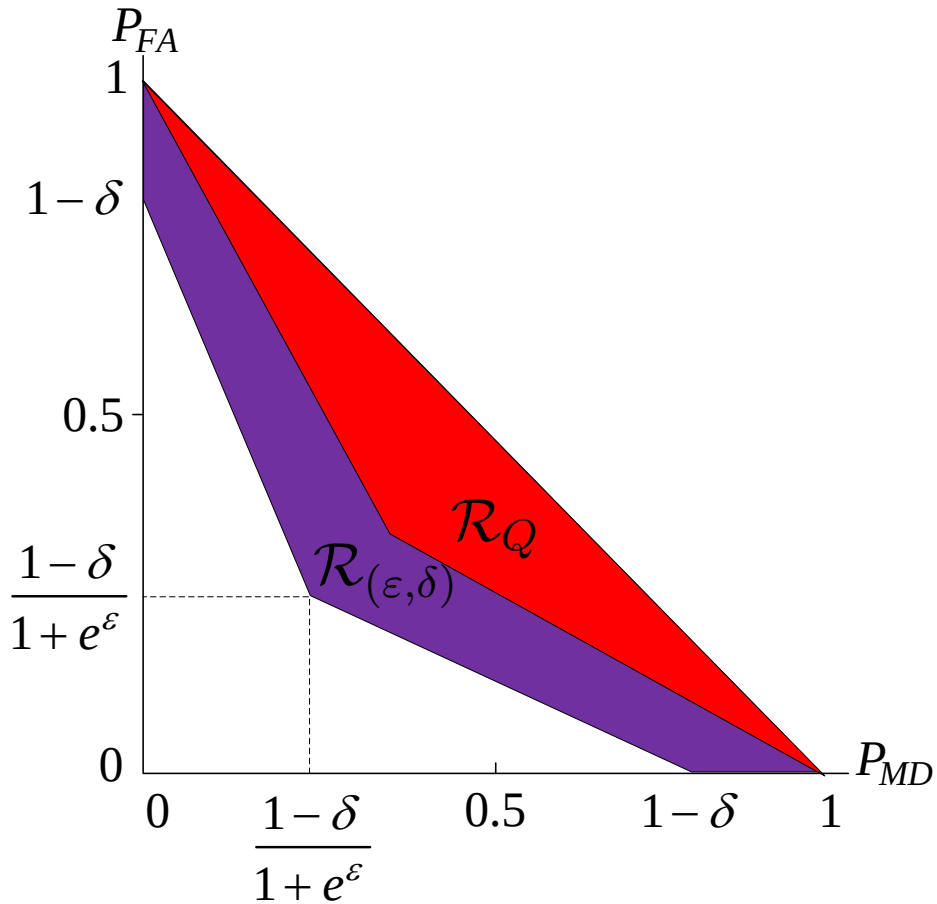


if $\mathcal{R}_2 \subset \mathcal{R}_1$, Q_2 guarantees **more privacy**

Local Differential Privacy (Binary Data)



Local Differential Privacy (Binary Data)



Q **is** (ε, δ)**-differentially private if** $\mathcal{R}_Q \subseteq \mathcal{R}_{(\varepsilon,\delta)}$

Local Differential Privacy

Q is ε-locally differentially private iff for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$

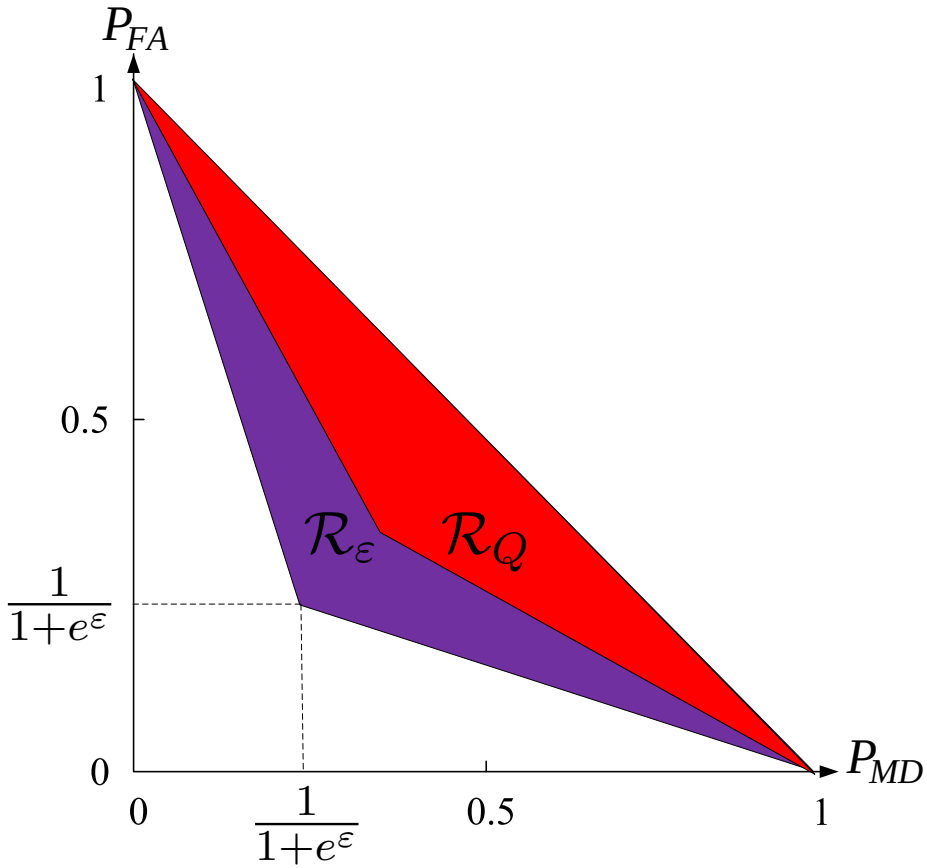
$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\varepsilon}$$

- ε **controls the level of privacy**
- $\varepsilon \downarrow \Longrightarrow$ **more private**
- $\varepsilon \uparrow \Longrightarrow$ **less private**

Local Differential Privacy

Q is ε-locally differentially private iff for all $x, x' \in \mathcal{X}$

$$\begin{aligned} P_{\mathrm{FA}} + e^{\varepsilon} P_{\mathrm{MD}} &\geq 1 \\ e^{\varepsilon} P_{\mathrm{FA}} + P_{\mathrm{MD}} &\geq 1 \end{aligned}$$



Q is ε-DP iff $\mathcal{R}_Q \subseteq \mathcal{R}_\varepsilon$ for all $x, x' \in \mathcal{X}$

Privacy vs. Utility

- the **more** private you want to be, the **less** utility you get
- there is a **fundamental trade-off** between **privacy** and **utility**

$$\begin{aligned} \underset{Q}{\text{maximize}} \quad & U(Q) \\ \text{subject to} \quad & Q \in \mathcal{D}_\varepsilon \end{aligned}$$

$U(Q)$: application dependent utility function

$\mathcal{D}_\varepsilon$: set of all ε-locally differentially private mechanisms

Summary of Results

Binary data: $|\mathcal{X}| = 2$

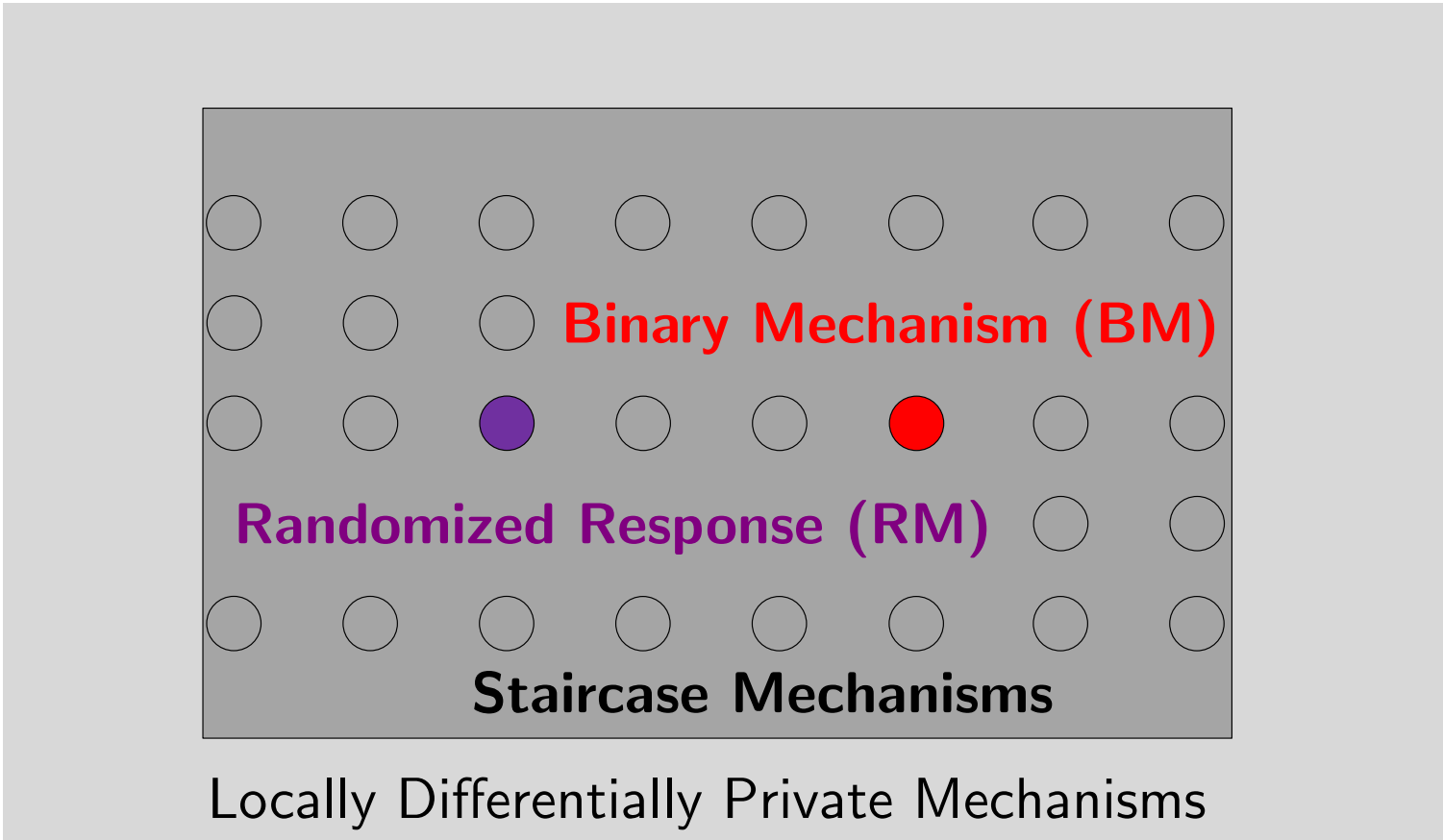
The Binary Randomized Response

w.p. $\frac{1}{1+e^{\varepsilon}}$ **lie** w.p. $\frac{e^{\varepsilon}}{1+e^{\varepsilon}}$ answer **truthfully**

- optimal for **all** ε
- optimal for **all** $U(Q)$ obeying the data processing inequality

Summary of Results

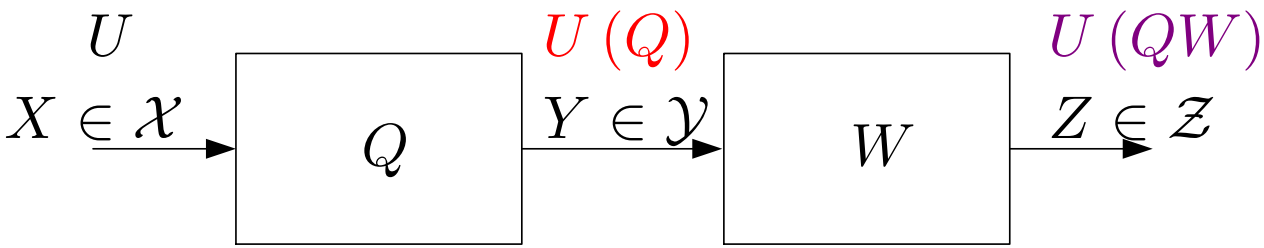
k-ary data: $|\mathcal{X}| = k > 2$



- staircase mechanisms are optimal for **all** ε and a **rich class of utilities**
- **BM** and **RR** are optimal in the **high** and **low** privacy regimes

CASE 1: BINARY DATA

Utility Functions



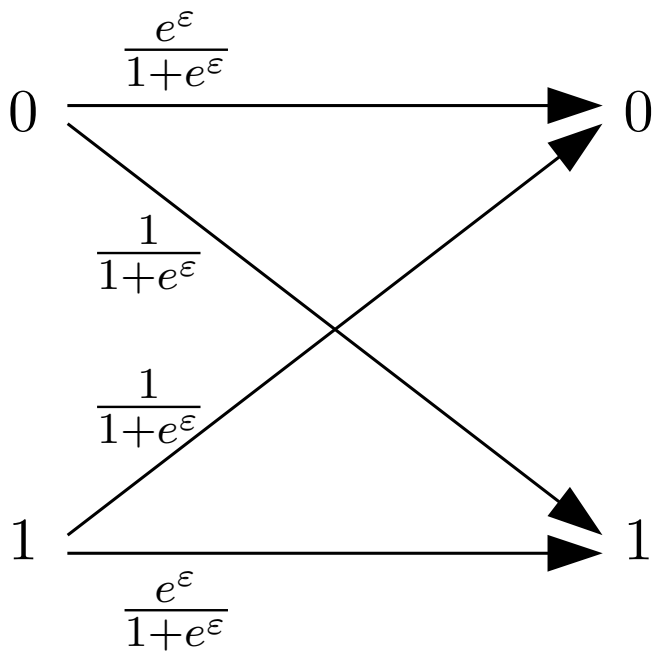
utility functions obeying the data processing inequality:

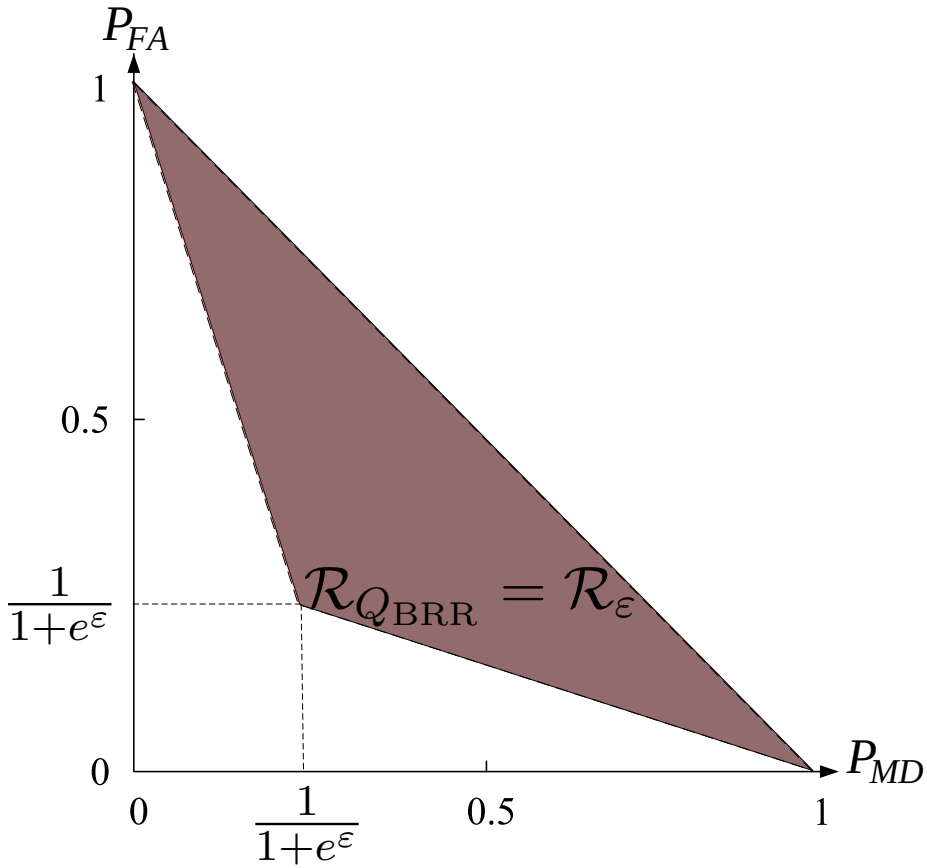
$$U(QW) \leq U(Q) \leq U$$

- further randomization can only reduce utility
- note: $Q \in \mathcal{D}_\varepsilon \implies QW \in \mathcal{D}_\varepsilon$

Main Result [Kairouz, et. al., 2014]

The **binary randomized response** is **optimal**





$\Longrightarrow$ $\forall U$ obeying the data processing inequality: $U(Q) \leq U(Q_{\mathrm{RR}})$

CASE 2: k-ARY DATA

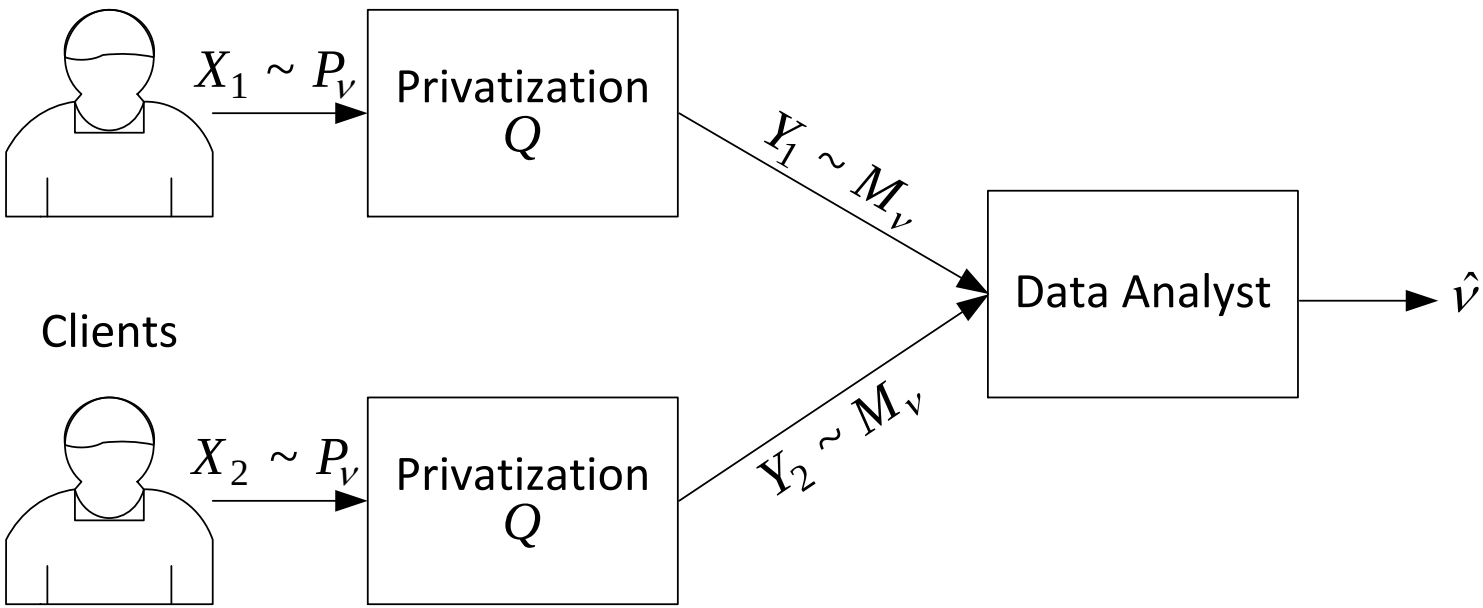
Information Theoretic Utility Functions

- $|\mathcal{X}| = k > 2$
- focus on a rich set of convex utility functions

$$\begin{aligned} \underset{Q}{\text{maximize}} \quad & U(Q) \\ \text{subject to} \quad & Q \in \mathcal{D}_\varepsilon \end{aligned}$$

includes all f-**divergences**, **mutual information**, etc.

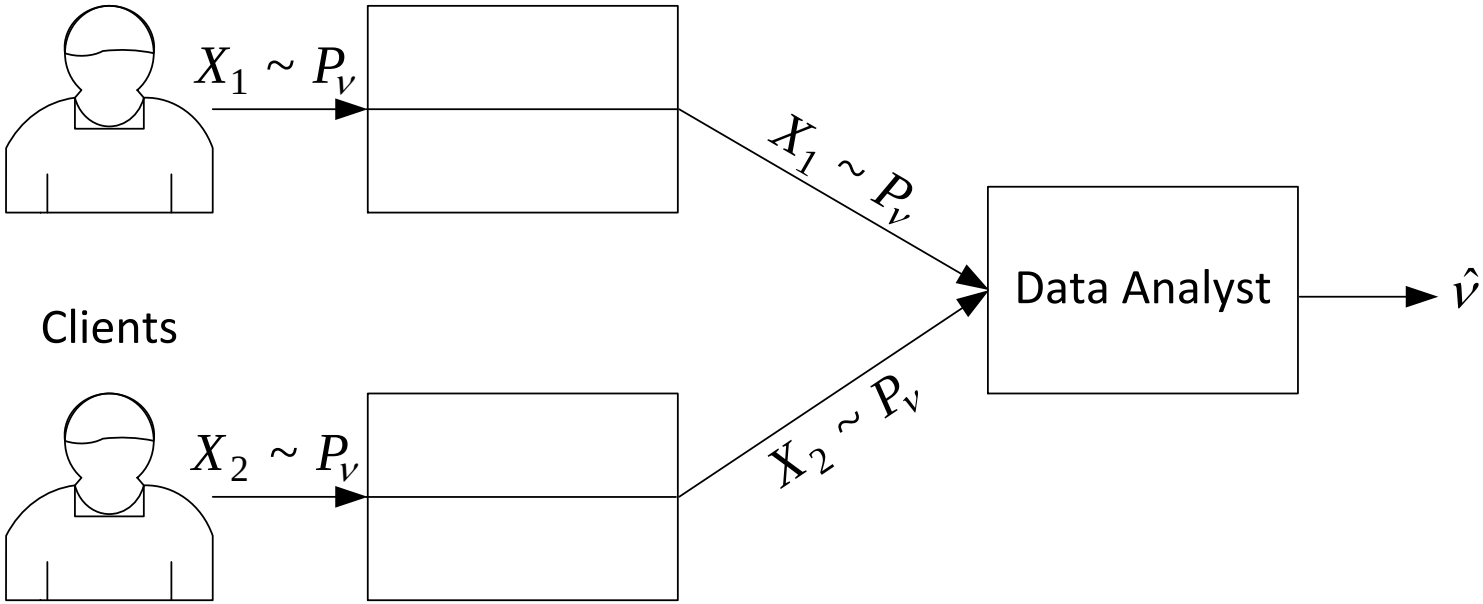
Statistical Data Model



analyst interested in **statistics** of data rather than **individual samples**

- **privatized data**: $Y_i \sim M_\nu(Y = y) = \sum_{x \in \mathcal{X}} Q(Y = y|x) P_\nu(X = x)$

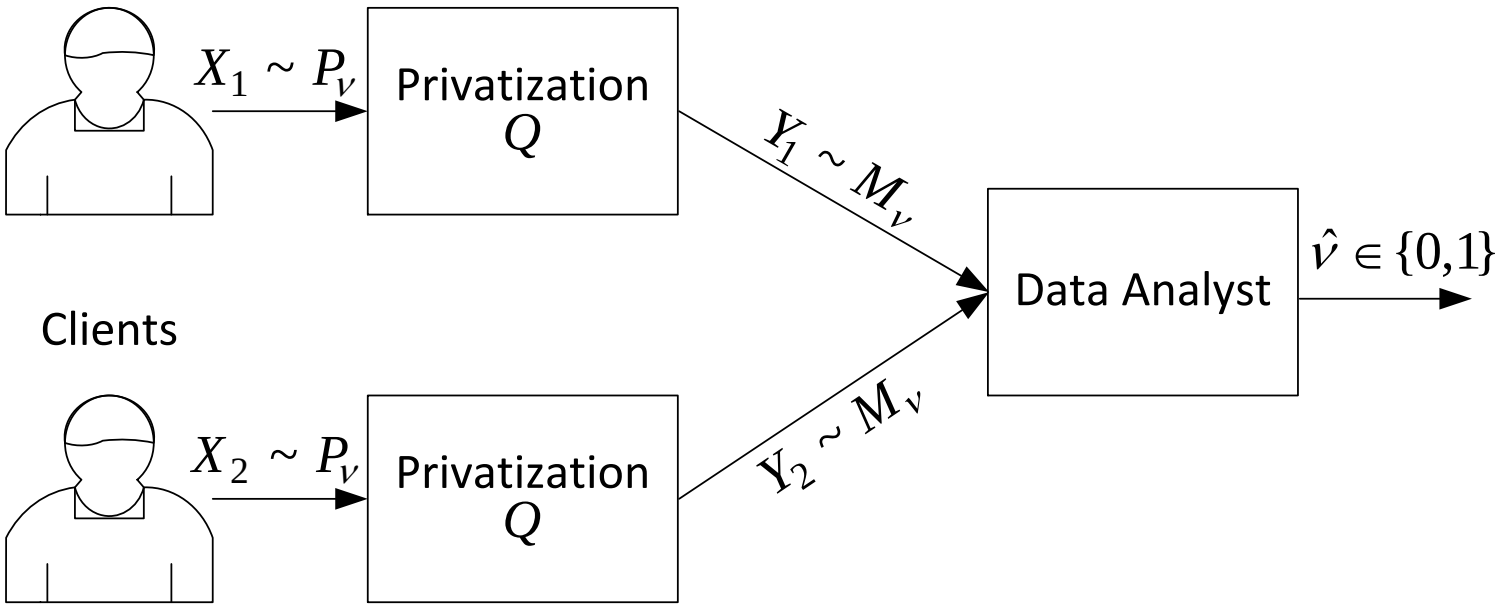
Hypothesis Testing



Given $\{X_i\}_{i=1}^n$, detect whether $\nu = 0$ or $\nu = 1$

- performance is a function of distance between P_0 from P_1
- Chernoff-Stein's lemma: $P_{\text{FA}} \approx e^{-n\, D_{\text{kl}}(P_0 || P_1)}$

Private Hypothesis Testing



Given $\{Y_i\}_{i=1}^n$, detect whether $\nu = 0$ or $\nu = 1$

- performance is a function of distance between M_0 from M_1
- Chernoff-Stein's lemma: $P_{\text{FA}} \approx e^{-n\, D_{\text{kl}}(M_0 || M_1)}$

f-Divergences

A rich family of measures of differences between distributions:

$$\begin{aligned} \underset{Q}{\text{maximize}} \quad & D_f(\underbrace{QP_0}_{M_0} \,\|\, \underbrace{QP_1}_{M_1}) \\ \text{subject to} \quad & Q \in \mathcal{D}_\varepsilon \end{aligned}$$

- KL divergence $D_{\mathrm{kl}}(M_0||M_1)$
- total variation $\|M_0 - M_1\|_{\mathrm{TV}}$
- **minimax rates** and **error exponents**

Staircase Mechanisms

Recall that:

Q is ε-locally differentially private iff for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$

$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\varepsilon}$$

ε controls the level of privacy

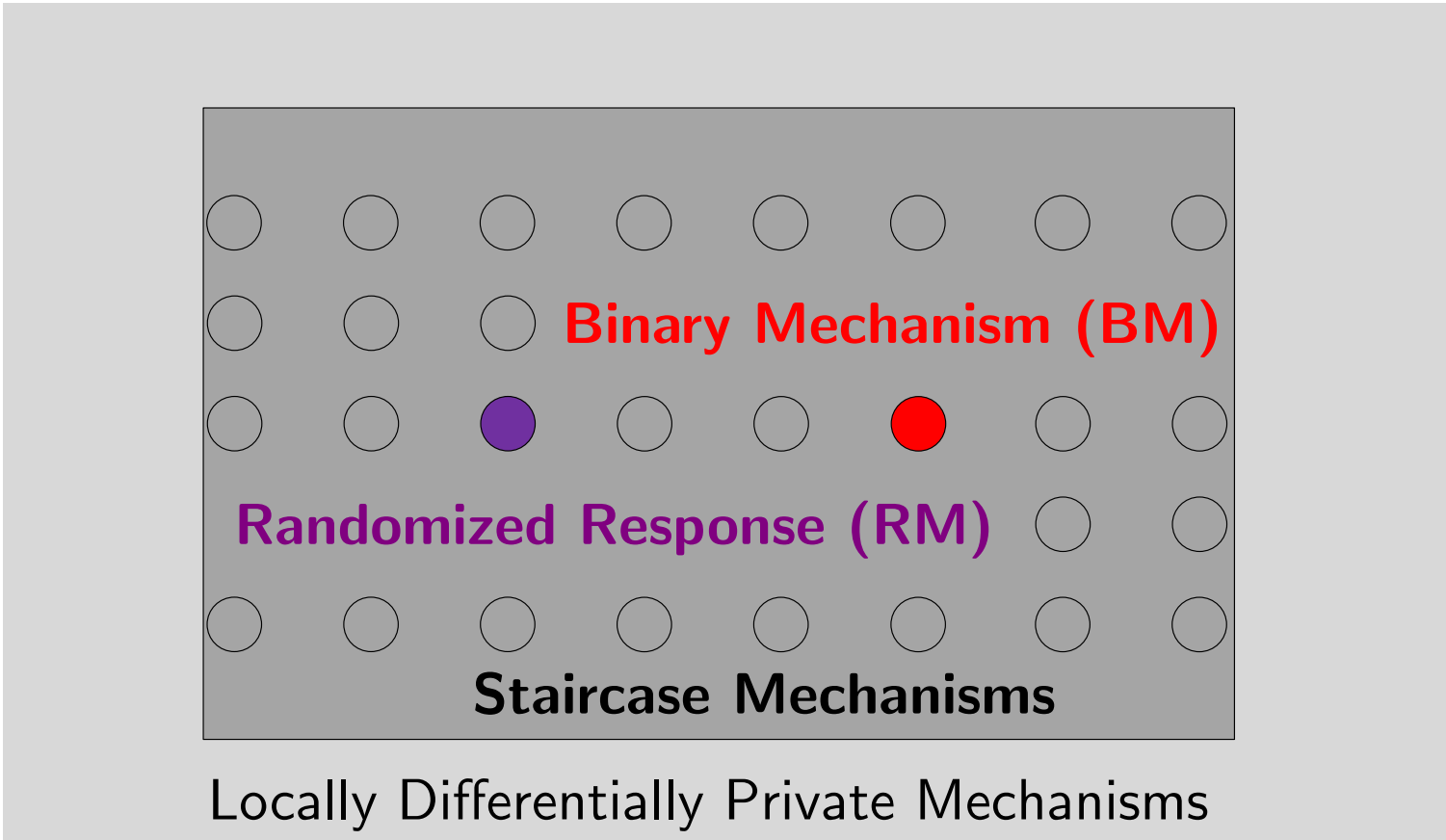
$\varepsilon \downarrow \implies$ **more private**

$\varepsilon \uparrow \implies$ **less private**

Staircase Mechanisms

Q is a **staircase mechanism** if for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$:

$$\frac{Q(y|x)}{Q(y|x')} \in \left\{e^{-\varepsilon}, 1, e^{\varepsilon}\right\}$$



Main Result [Kairouz, et. al., 2014]

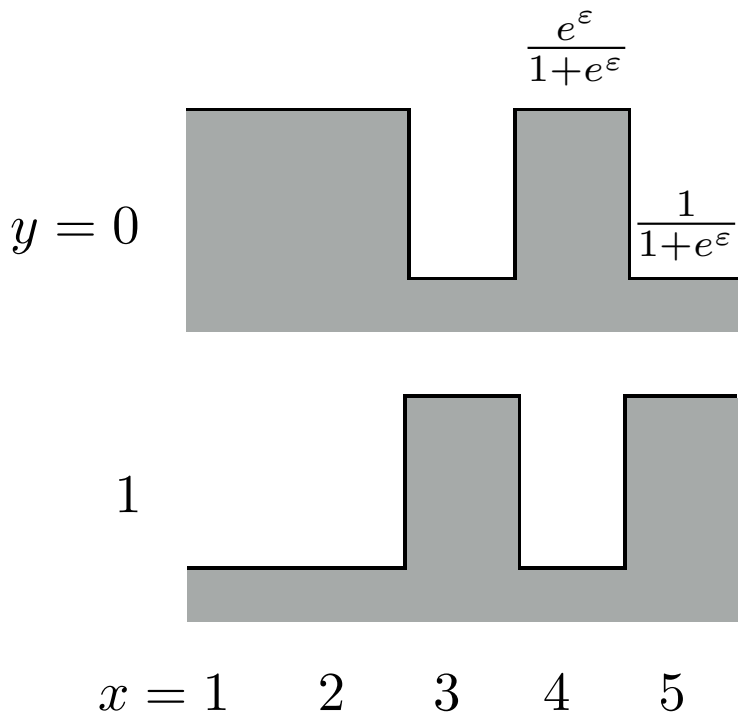
$$\underset{Q}{\text{maximize}} \quad D_f(\underbrace{QP_0}_{M_0} \,\|\, \underbrace{QP_1}_{M_1}) \quad = \quad \underset{Q}{\text{maximize}} \quad D_f(\underbrace{QP_0}_{M_0} \,\|\, \underbrace{QP_1}_{M_1})$$

$$\text{subject to} \quad Q \in \mathcal{D}_\varepsilon \qquad\qquad \text{subject to} \quad Q \in \mathcal{S}_\varepsilon$$

$\mathcal{S}_\varepsilon$: set of all **staircase mechanisms** with $|\mathcal{Y}| \leq |\mathcal{X}|$

- **staircase** mechanisms are **optimal**
- no gain in **larger output alphabets**
- there are **finitely many** staircase mechanisms
- same result holds for a rich set of convex utility functions

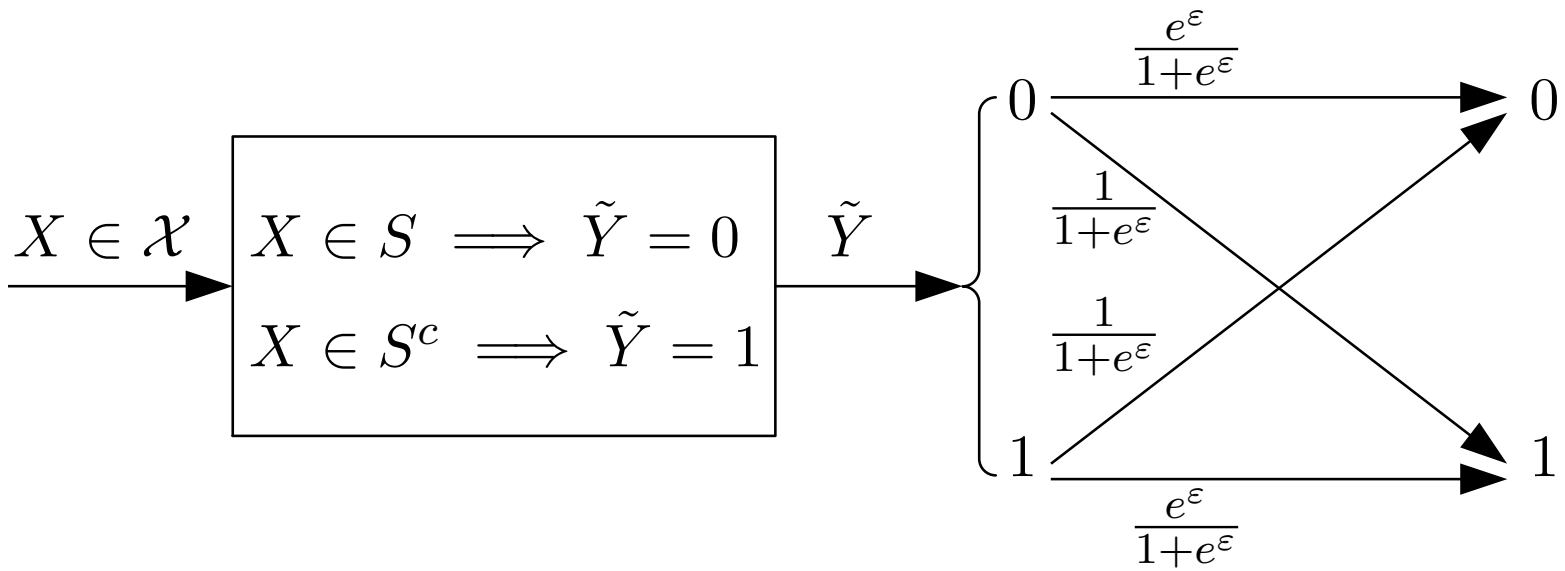
Binary Mechanisms



- maps k-ary inputs to binary outputs

Binary Mechanisms

A **deterministic** binary mapping followed by a **randomized response**



- a highly quantized version of the original data

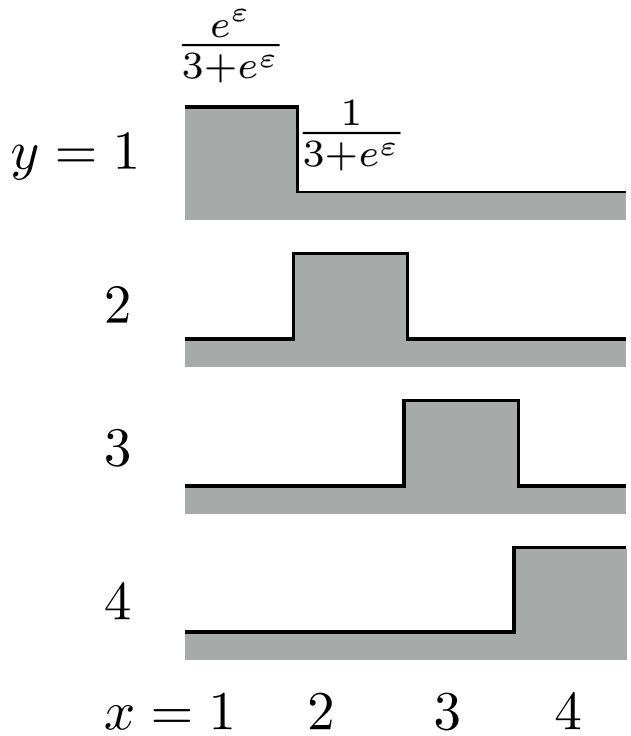
Optimality of Binary Mechanisms (High Privacy)

$$Q_{\mathrm{B}}(0|x) = \begin{cases} \frac{e^{\varepsilon}}{1+e^{\varepsilon}} & \text{if } P_0(x) \geq P_1(x) \\ \frac{1}{1+e^{\varepsilon}} & \text{if } P_0(x) < P_1(x) \end{cases}$$

$$Q_{\mathrm{B}}(1|x) = \begin{cases} \frac{e^{\varepsilon}}{1+e^{\varepsilon}} & \text{if } P_0(x) < P_1(x) \\ \frac{1}{1+e^{\varepsilon}} & \text{if } P_0(x) \geq P_1(x) \end{cases}$$

$\forall\ P_0, P_1,\ \exists\ \underline{\varepsilon}(P_0, P_1) > 0$ such that $\forall \varepsilon \leq \underline{\varepsilon}(P_0, P_1)$, Q_{B} is **optimal**

Randomized Response



- maps k-ary inputs to k-ary outputs

Randomized Response

w.p. $\frac{|\mathcal{X}|-1}{|\mathcal{X}|-1+e^{\varepsilon}}$ **lie** w.p. $\frac{e^{\varepsilon}}{|\mathcal{X}|-1+e^{\varepsilon}}$ answer **truthfully**

- **lie** $=$ choose another character in $\mathcal{X}$ uniformly at random
- can be viewed as a k-ary extension to the binary randomized response

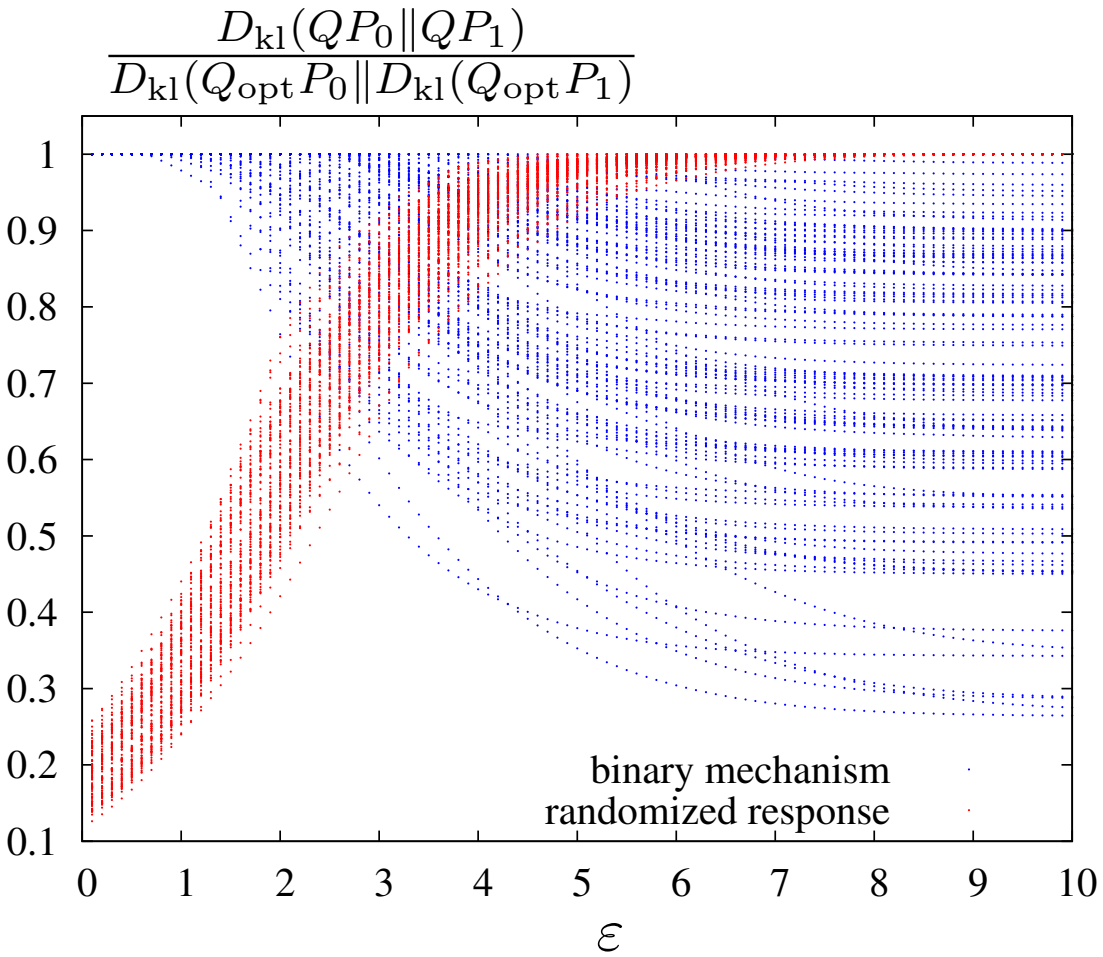
Optimality of Randomized Response (Low Privacy)

$$Q_{\mathrm{RR}}(y|x) = \begin{cases} \frac{e^{\varepsilon}}{|\mathcal{X}|-1+e^{\varepsilon}} & \text{if } y = x \\ \frac{1}{|\mathcal{X}|-1+e^{\varepsilon}} & \text{if } y \neq x \end{cases}$$

$\forall\ P_0, P_1,\ \exists\ \overline{\varepsilon}(P_0, P_1) > 0$ such that $\forall \varepsilon \geq \overline{\varepsilon}(P_0, P_1)$, Q_{RR} is **optimal**

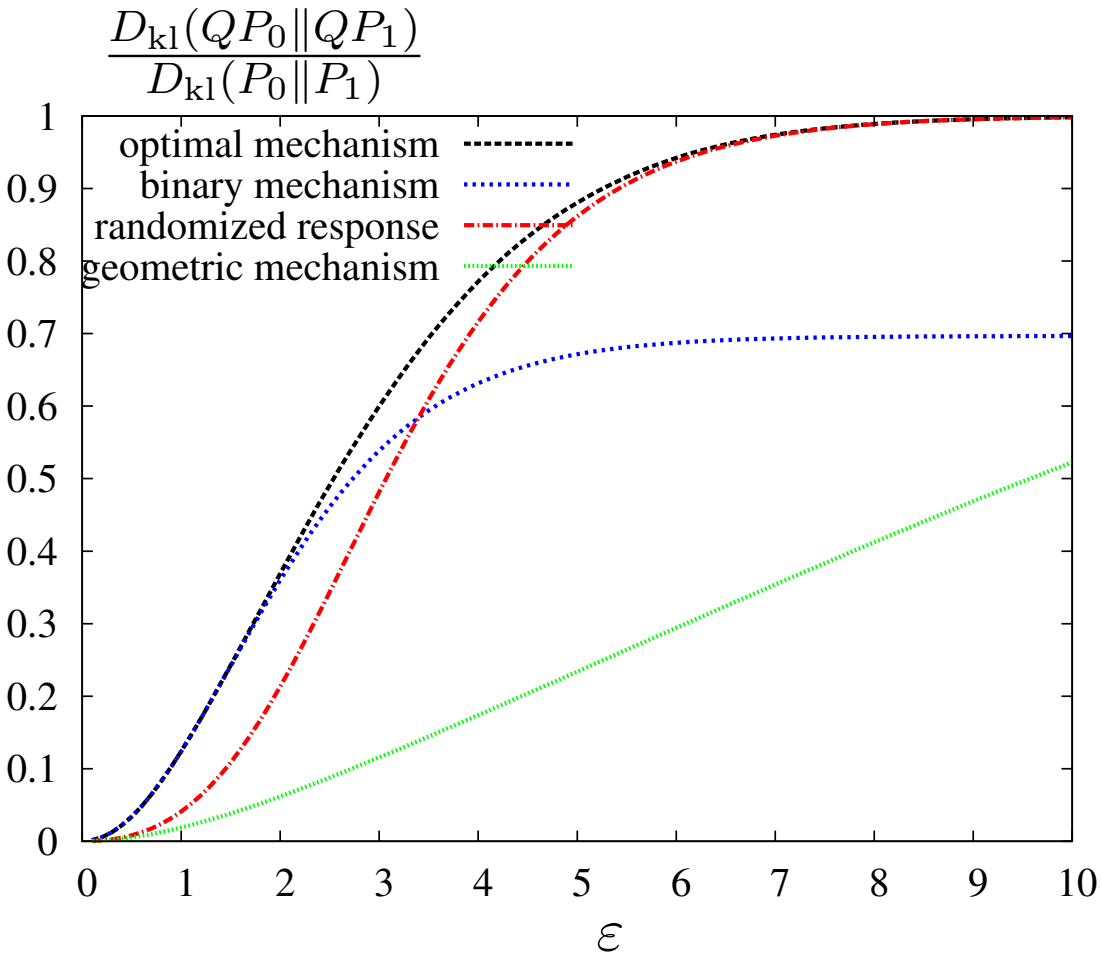
- note that Q_{RR} does not depend on P_0 and P_1

Numerical Example for KL Divergence



- $|\mathcal{X}| = 6$
- 100 random pairs of (P_0, P_1)

Numerical Example for KL Divergence



- $|\mathcal{X}| = 6$
- averaged over 100 random pairs of (P_0, P_1)

Big Picture

- local differential privacy is **crucial** for data collection applications
- we studied a broad class of information theoretic utilities
- we provided **explicit constructions** of **optimal mechanisms**
- more results on local privacy:
  - *"Extremal mechanisms for local differential privacy"*, NIPS 2014
  - *"The composition theorem for differential privacy"*, ICML 2015
  - *"Optimality of non-interactive randomized response"*, arXiv:1407.1546

Big Picture

- local differential privacy is **crucial** for data collection applications
- we studied a broad class of information theoretic utilities
- we provided **explicit constructions** of **optimal mechanisms**
- more results on local privacy:
  - *"Extremal mechanisms for local differential privacy"*, NIPS 2014
  - *"The composition theorem for differential privacy"*, ICML 2015
  - *"Optimality of non-interactive randomized response"*, arXiv:1407.1546

Big Picture

- local differential privacy is **crucial** for data collection applications
- we studied a broad class of information theoretic utilities
- we provided **explicit constructions** of **optimal mechanisms**
- more results on local privacy:
  - *"Extremal mechanisms for local differential privacy"*, NIPS 2014
  - *"The composition theorem for differential privacy"*, ICML 2015
  - *"Optimality of non-interactive randomized response"*, arXiv:1407.1546

Big Picture

- local differential privacy is **crucial** for data collection applications
- we studied a broad class of information theoretic utilities
- we provided **explicit constructions** of **optimal mechanisms**
- more results on local privacy:
  - *"Extremal mechanisms for local differential privacy"*, NIPS 2014
  - *"The composition theorem for differential privacy"*, ICML 2015
  - *"Optimality of non-interactive randomized response"*, arXiv:1407.1546

Going Forward

- private **green button**
- private **genomic data sharing**
- private **RAPPOR**

Thank You
Questions?