The Optimal Mechanism in Differential Privacy

Quan Geng

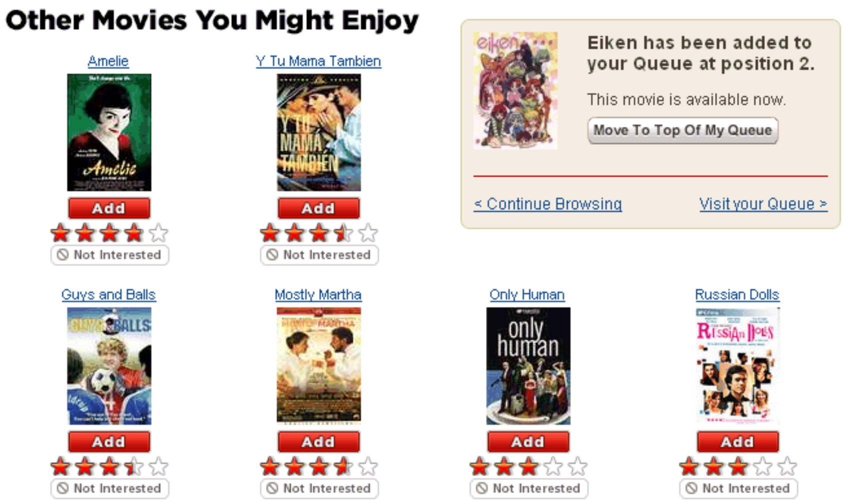
Advisor: Prof. Pramod Viswanath

Outline

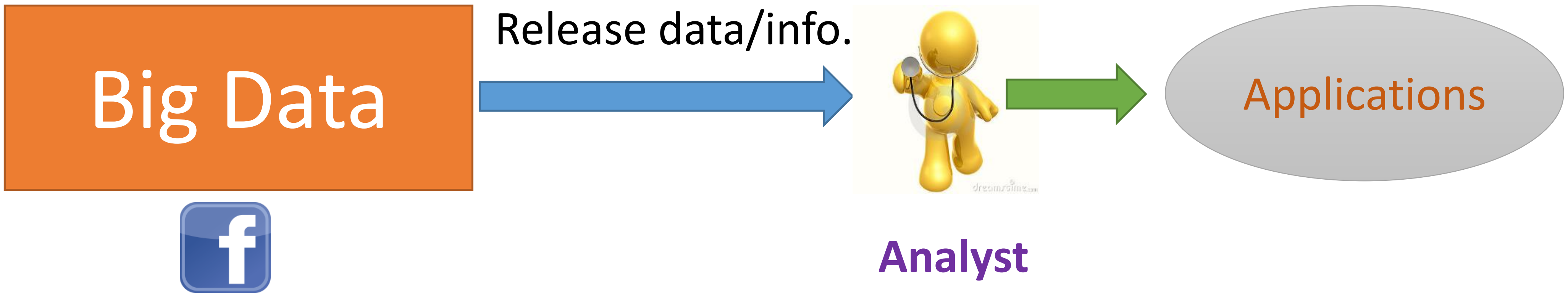
- Background on differential privacy
- Problem formulation
- Main result on the optimal mechanism
- Extensions to other settings
- Conclusion and future work

Motivation

- Vast amounts of personal information are collected
- Data analysis produces a lot of useful applications



Motivation



- How to release the data while protecting individual's privacy?

Motivation: Netflix Prize

- (2006) Netflix hosted a contest to improve movie recommendation
- Released dataset
  - 100 million ratings
  - 500 thousand users
  - 18 thousand movies

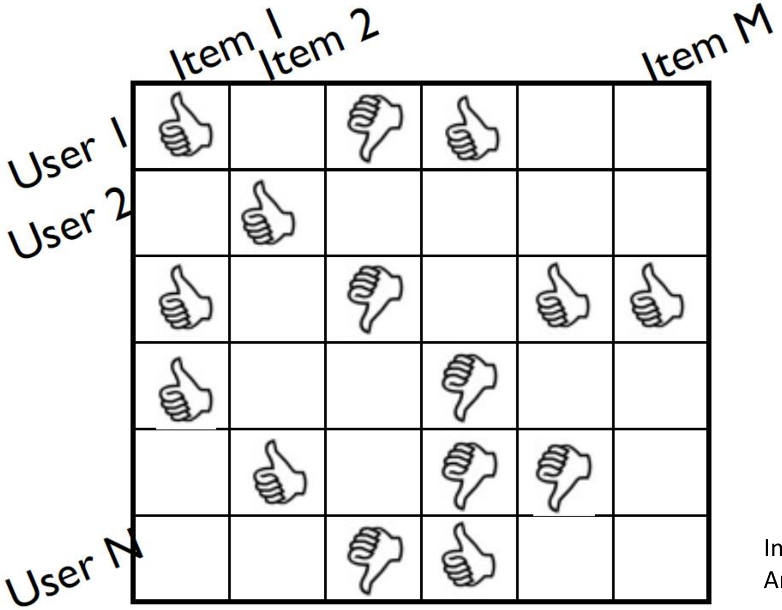


Image Credit:
Arvind Narayanan

Motivation: Netflix Prize

- (2006) Netflix hosted a contest to improve movie recommendation
- Released dataset
  - 100 million ratings
  - 500 thousand users
  - 18 thousand movies
- Anonymization to protect customer privacy

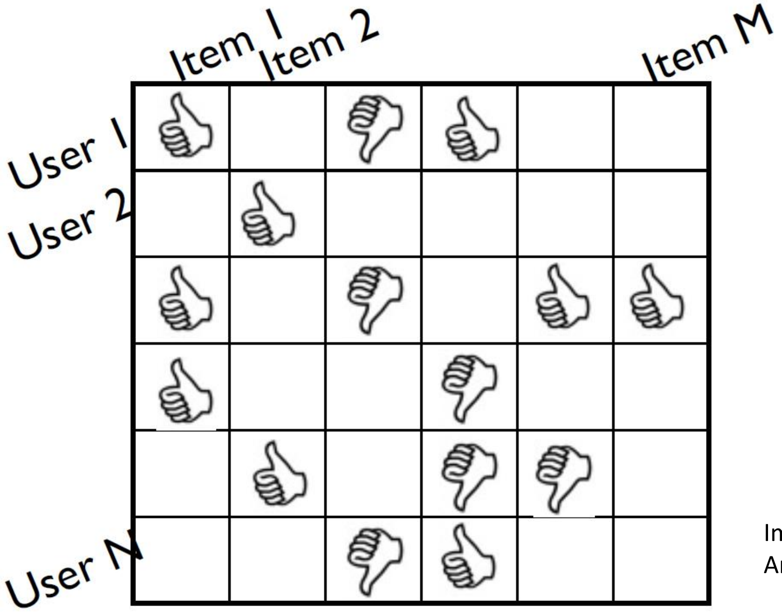
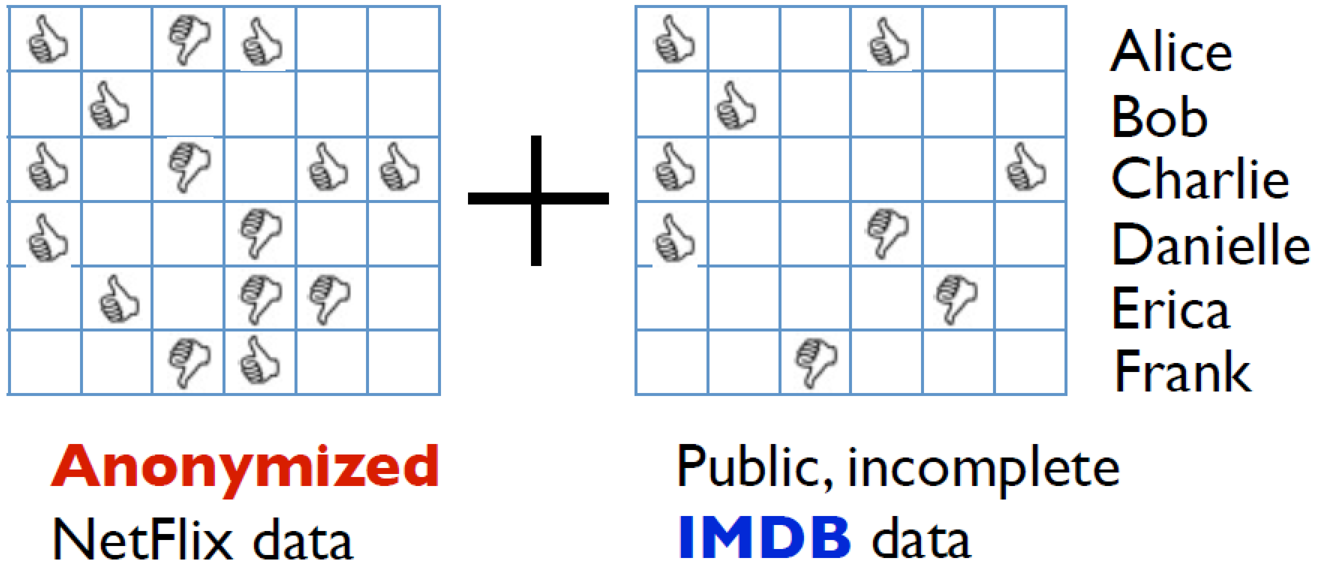


Image Credit:
Arvind Narayanan

Motivation: Netflix Prize Dataset Release



[Narayanan, Shmatikov 2008]

Image Credit:
Arvind Narayanan

Motivation

- How to protect PRIVACY resilient to attacks with arbitrary side information?

Motivation

- How to protect PRIVACY resilient to attacks with arbitrary side information?
    - **Ans: randomized releasing mechanism**

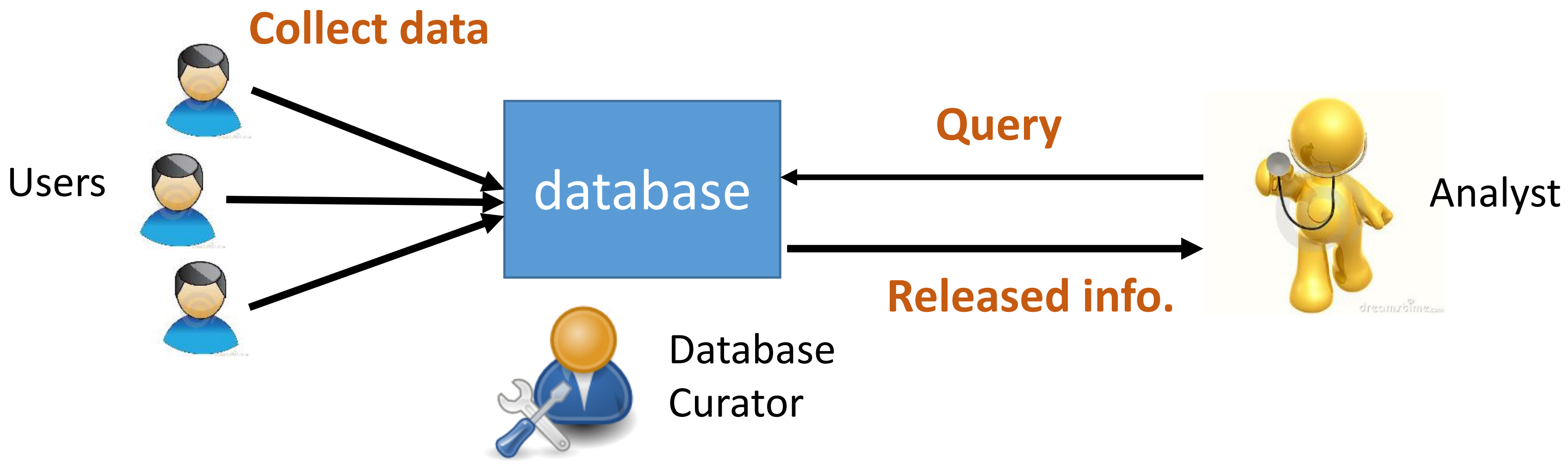
Motivation

- How to protect PRIVACY resilient to attacks with arbitrary side information?
    - **Ans:** **randomized releasing mechanism**
- How much randomness is needed?
    - completely random (no utility)
    - deterministic (no privacy)

Motivation

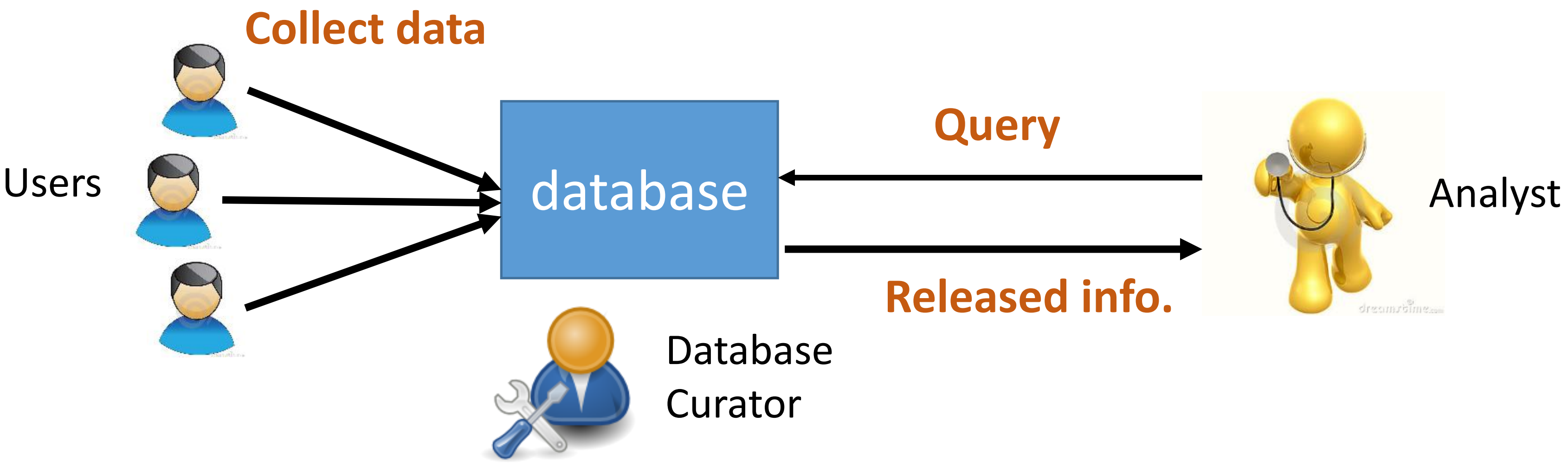
- How to protect PRIVACY resilient to attacks with arbitrary side information?
  - **Ans: randomized releasing mechanism**
- How much randomness is needed?
  - completely random (no utility)
  - deterministic (no privacy)
- **Differential Privacy** [Dwork et. al. 06]: one way to quantify the level of randomness and privacy

Background on Differential Privacy



- **Database Curator**: How to **answer** a query, providing **useful** data information to the analyst, while still protecting the **privacy** of each user.

Background on Differential Privacy



dataset: D

Age
A: 20
B: 35
C: 43
D: 30

query function: q (D)

q: How many people are older than 32?

q(D) = 2

randomized released mechanism: $\mathrm{K(D)}$

K(D) = 1 w.p. 1/8
K(D) = 2 w.p. 1/2
K(D) = 3 w.p. 1/4
K(D) = 4 w.p. 1/8

Background on Differential Privacy

- **Two neighboring datasets**: differ only at one element

Age
A: 20
B: 35
C: 43
D: 30

D_1

Age
A: 20
B: 35
D: 30

D_2

Background on Differential Privacy

- **Two neighboring datasets**: differ only at one element

Age
A: 20
B: 35
C: 43
D: 30

D_1

Age
A: 20
B: 35
D: 30

D_2

$$K(D_1) \approx K(D_2)$$

Differential Privacy: **presence** or **absence** of any individual record in the dataset should not affect the released information significantly.

Background on Differential Privacy

- A randomized mechanism K gives **ϵ-differential privacy**, if for any two neighboring datasets D_1, D_2 , and all S ⊂Range(K),

$$\mathbf{Pr(K(D_1) \in S) \leq e^{\epsilon}\, Pr(K(D_2) \in S)}$$

(make hypothesis testing hard)

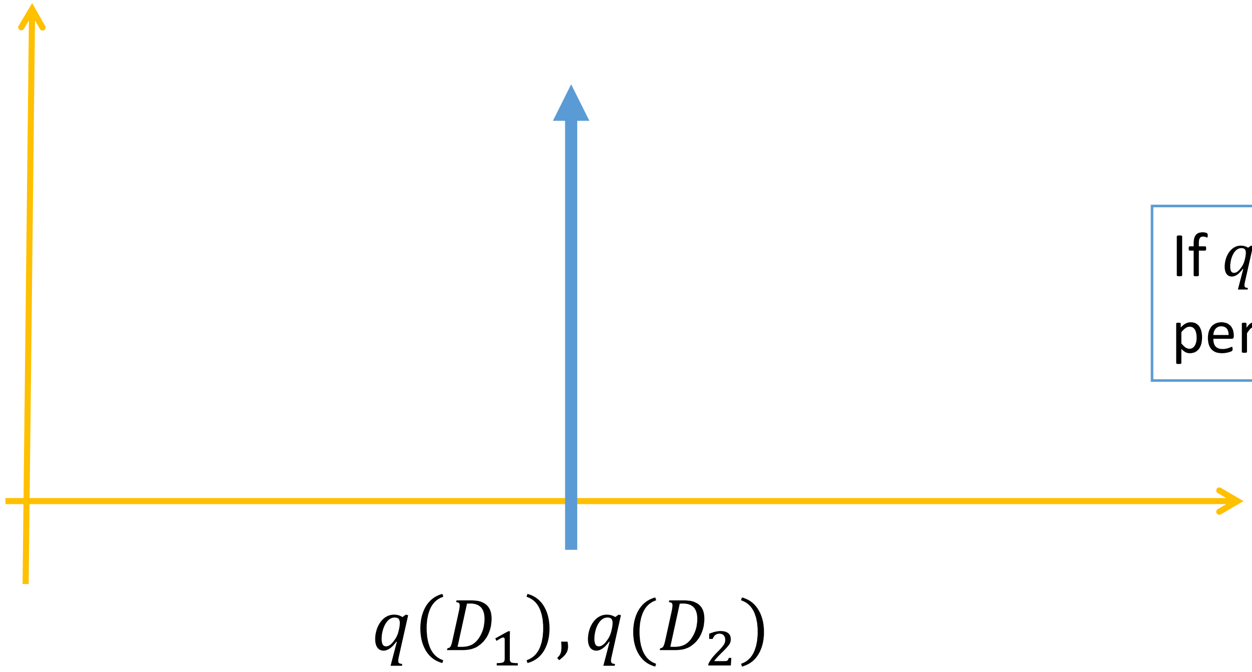
- ϵ quantifies the level of privacy
  - $\epsilon \to 0$, high privacy
  - $\epsilon \to +\infty$, low privacy
  - a **social** question to choose ϵ (can be 0.01, 0.1, 1, 10 …)

Background on Differential Privacy

- Q: How much perturbation needed to achieve ϵ-DP?
- A: depends on how different $q(D_1), q(D_2)$ are

Background on Differential Privacy

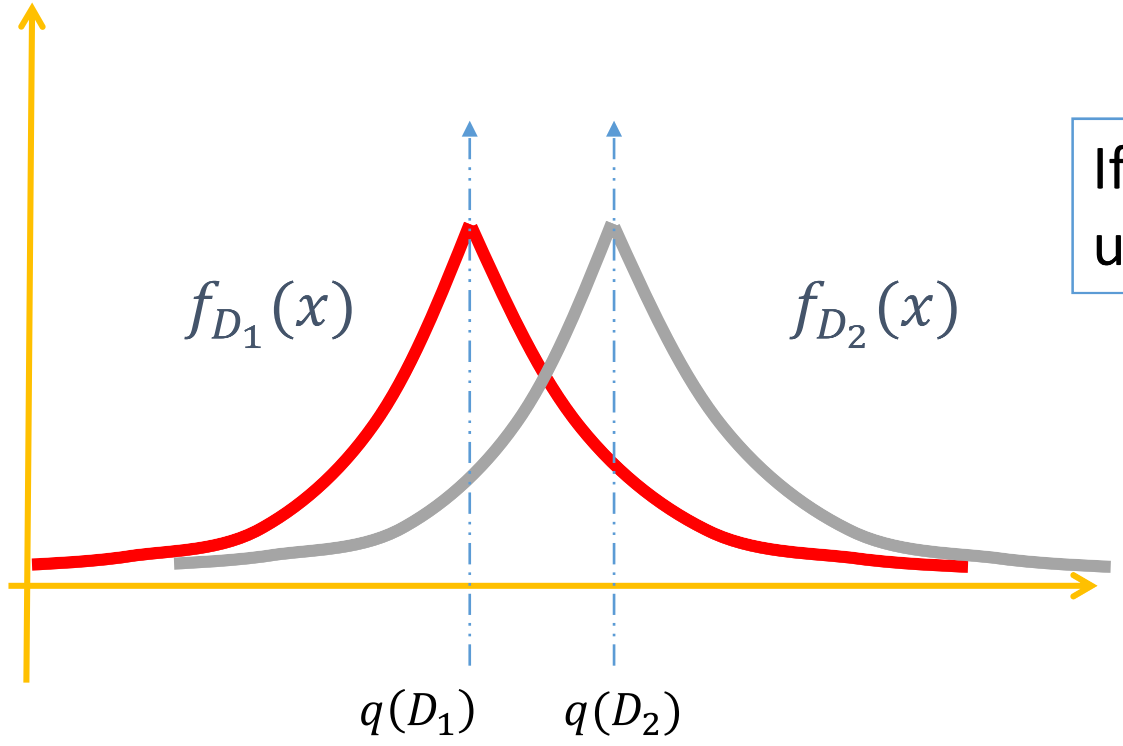
- Q: How much perturbation needed to achieve ϵ-DP?
- A: depends on how different $q(D_1), q(D_2)$ are



If $q(D_1) = q(D_2)$, no perturbation is needed.

Background on Differential Privacy

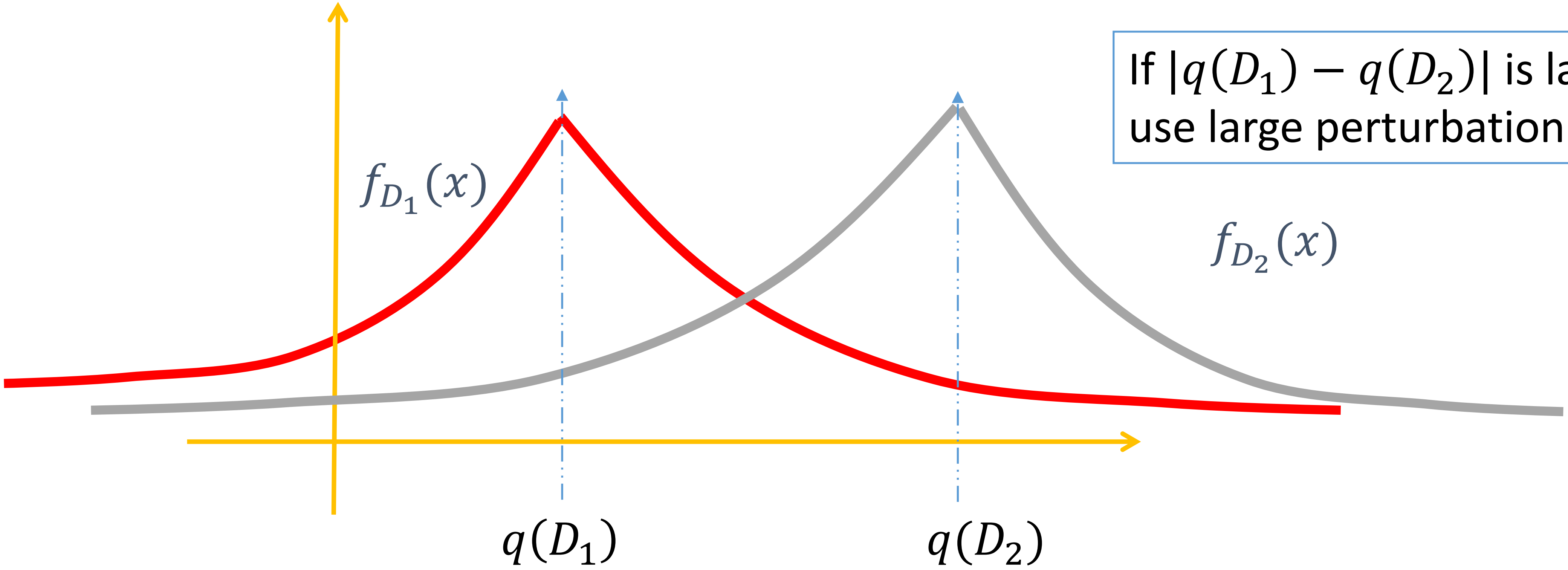
- Q: How much perturbation needed to achieve ϵ-DP?
- A: depends on how different $q(D_1), q(D_2)$ are



If $|q(D_1) - q(D_2)|$ is small, use small perturbation

Background on Differential Privacy

- Q: How much perturbation needed to achieve ϵ-DP?
- A: depends on how different $q(D_1), q(D_2)$ are



If $|q(D_1) - q(D_2)|$ is large, use large perturbation

Background on Differential Privacy

- **Global Sensitivity** Δ: how different when q is applied to neighboring datasets

$$\boldsymbol{\Delta} \coloneqq \max_{(D_1, D_2)\ are\ neighbors} |q(D_1) - q(D_2)|$$

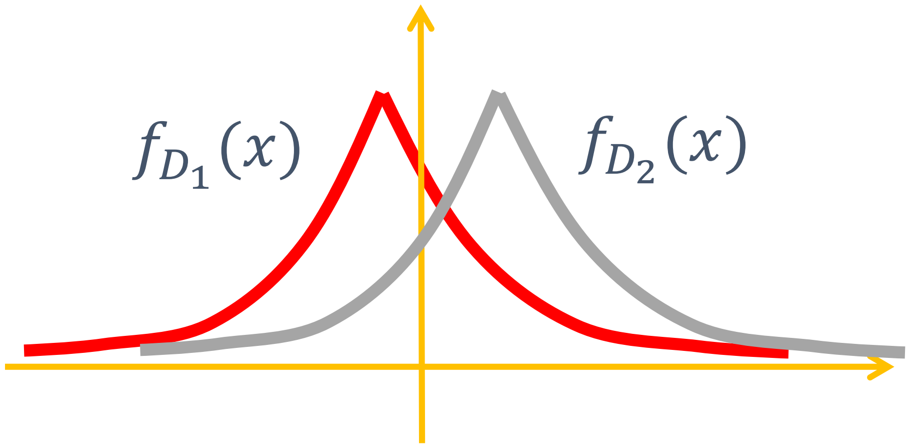
- Example: for a count query, $\Delta = 1$

Background on Differential Privacy

- Laplace Mechanism:

$$K(D) = q(D) + Lap(\frac{\Delta}{\epsilon}),$$

$Lap\left(\frac{\Delta}{\epsilon}\right)$ is a r.v. with p.d.f $f(x) = \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}}, \;\; \lambda = \frac{\Delta}{\epsilon}$



- Basic tool in DP

Optimality of Existing work?

- Laplace Mechanism:

$$\boldsymbol{K(D) = q(D) + Lap}\left(\frac{\Delta}{\epsilon}\right),$$

- Two Questions:
  - Is **data-independent** perturbation optimal?
  - Assume data-independent perturbation, is **Laplacian** distribution optimal?

Optimality of Existing work?

- Laplace Mechanism:

$$\boldsymbol{K(D) = q(D) + Lap(\frac{\Delta}{\epsilon})},$$

- Two questions:
  - Is **data-independent** perturbation optimal?
  - Assume data-independent perturbation, is **Laplacian** distribution optimal?

- Our results:
  - **data-independent** perturbation is optimal
  - **Laplacian** distribution is not optimal: the optimal is **staircase** distribution

Problem Formulation: DP constraint

- A generic randomized mechanism K is a family of noise probability measures (t is query output)

$$\boldsymbol{K = \{\nu_t : t \in R\}}$$

- **DP constraint:** $\forall t_1, t_2 \in R, s.t. |t_1 - t_2| \leq \Delta,$
  $\boldsymbol{\nu_{t_1}(S) \leq e^{\epsilon}\nu_{t_2}(S + t_1 - t_2)}, \forall \text{measurable set } S$

Problem Formulation: utility (cost) model

- Cost function on the noise

$$L: R \to R$$

- Given query output t,

$$\text{Cost}(\nu_t) = \int L(x)\nu_t(dx)$$

- Example
  - $L(x) = |x|$, noise magnitude
  - $L(x) = |x|^2$, noise power

- **Objective**(minmax):

$$\text{minimize} \sup_{t \in R} \int_{x \in R} L(x)\nu_t(dx)$$

Problem Formulation: put things all together

$$Minimize \sup_{t \in R} \int_{x \in R} L(x) \nu_t(dx)$$

s.t. $\boldsymbol{\nu}_{t_1}(S) \le e^{\epsilon} \boldsymbol{\nu}_{t_2}(S + t_1 - t_2),$

$\forall \text{measurable set } S, \forall t_1, t_2 \in R, \text{s.t.} |t_1 - t_2| \le \Delta,$

Main Result: $\nu_t = \nu$

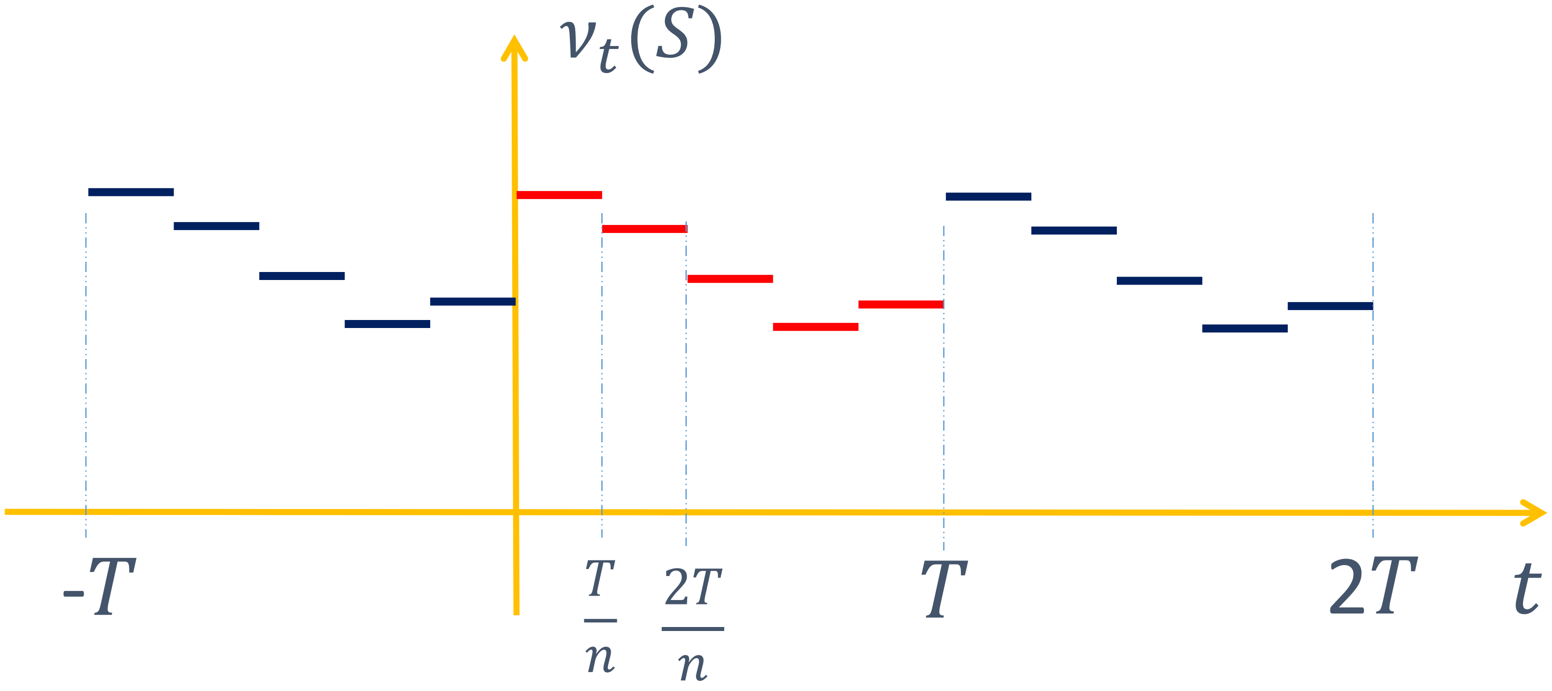
In the optimal mechanism, ν_t is **independent** of t (under a technical condition).

Main Result: $\nu_t = \nu$

In the optimal mechanism, ν_t is **independent** of t (under a technical condition).

Piecewise constant over t

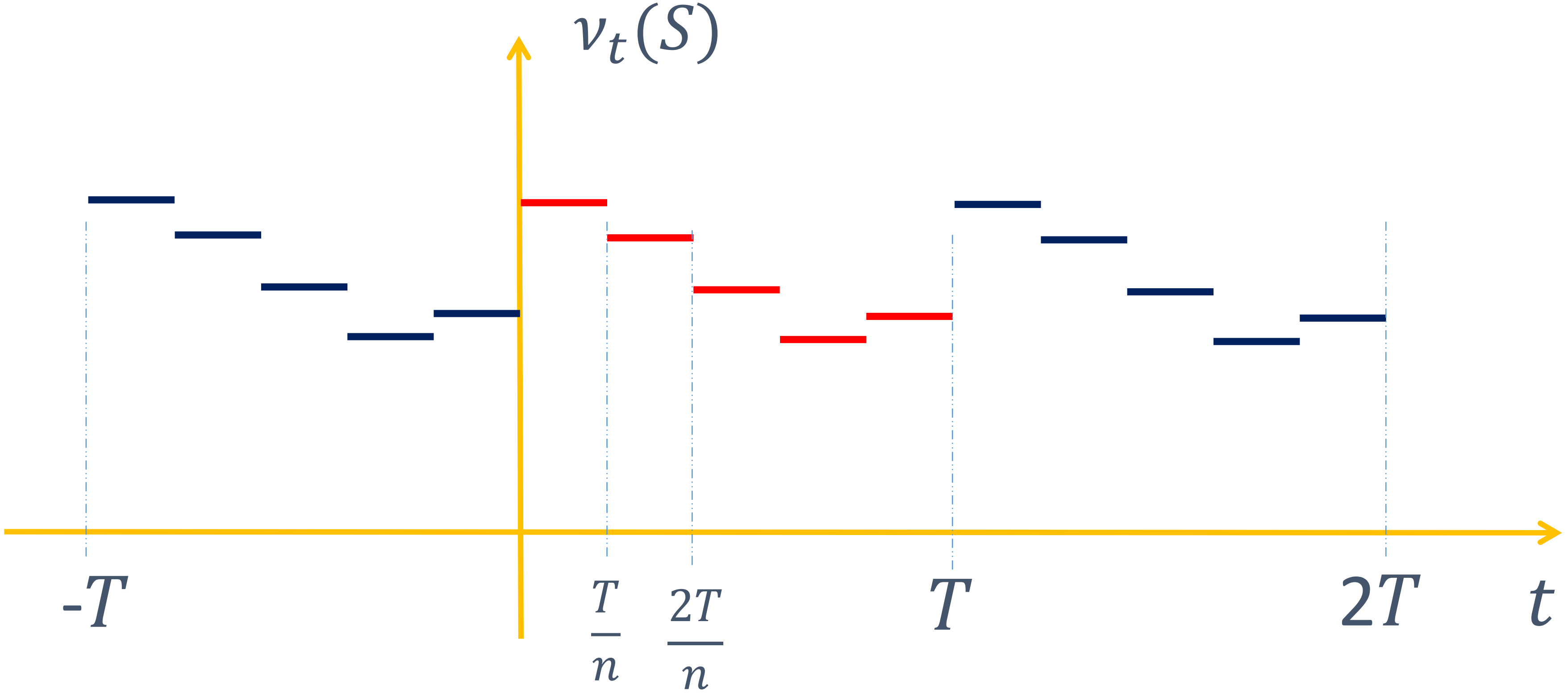
Periodic over t



Main Result: $\nu_t = \nu$

Piecewise constant over t

Periodic over t



In the optimal mechanism among $\cup_{T>0} \cup_{n \geq 1} K_{T,n}$,

ν_t is **independent** of t

Optimal noise probability distribution

$$\boldsymbol{K(D) = q(D) + X},$$

$$\begin{aligned} &\text{Minimize} \quad \int L(x)P(dx) \\ &\text{s.t.} \quad \Pr(X \in S) \le e^{\epsilon} \Pr(X \in S + d), \\ &\forall |d| \le \Delta, \text{measurable set } S \end{aligned}$$

Optimal noise probability distribution

$$\boldsymbol{K(D) = q(D) + X},$$

$$\text{Minimize} \quad \int L(x)P(dx)$$

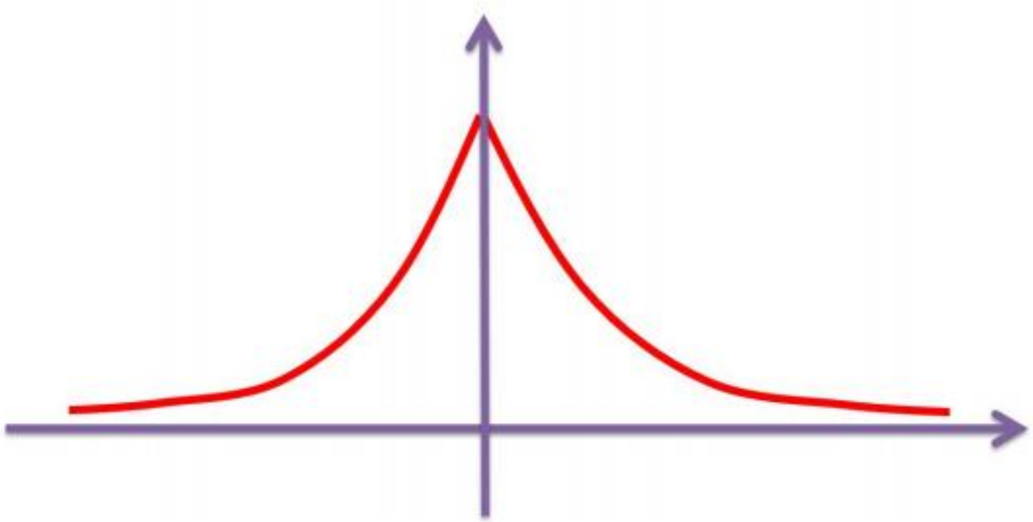
$$\text{s.t.} \qquad \Pr(X \in S) \le e^{\epsilon} \Pr(X \in S + d),$$

$$\forall |d| \le \Delta, \text{measurable set } S$$

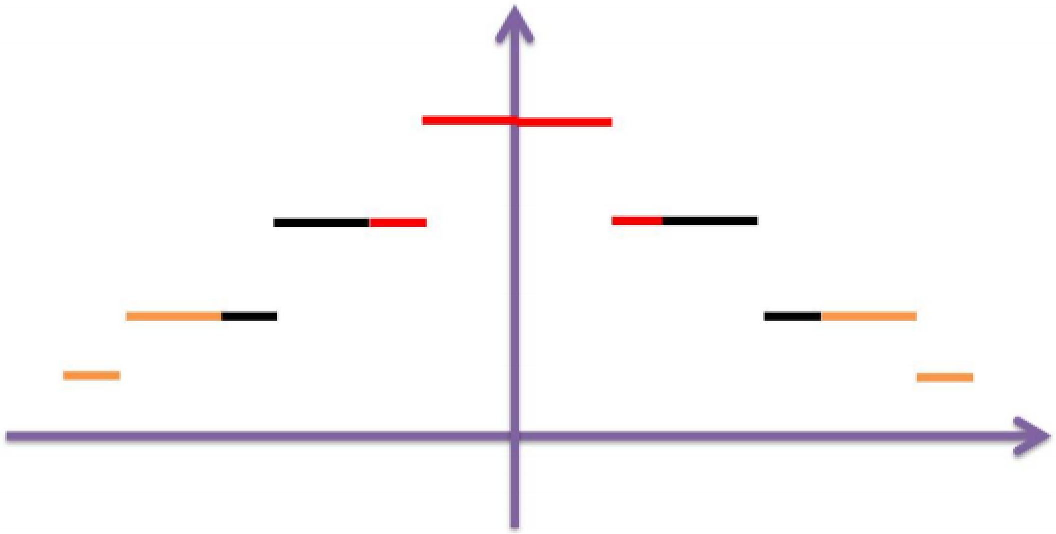
- $L(x)$ satisfies:
  - symmetric, and increasing of $|x|$
  - $\sup \frac{L(T+1)}{L(T)} < +\infty$

Main Result

The optimal probability distribution has staircase-shaped p.d.f.



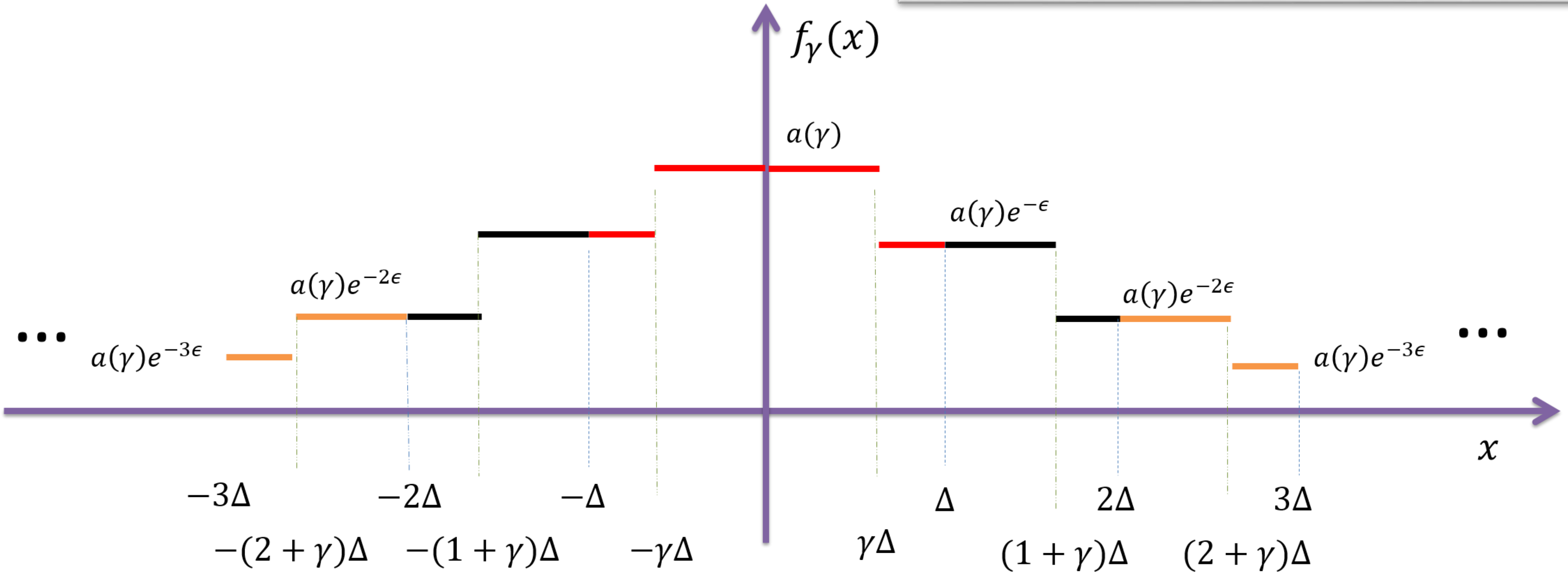
(a) Laplace Mechanism



(b) Staircase Mechanism

Main Result

$$f_\gamma(x) = \begin{cases} a(\gamma) & x \in [0, \gamma\Delta) \\ e^{-\epsilon} a(\gamma) & x \in [\gamma\Delta, \Delta) \\ e^{-k\epsilon} f_\gamma(x - k\Delta) & x \in [k\Delta, (k+1)\Delta) \\ f_\gamma(-x) & x < 0 \end{cases}$$

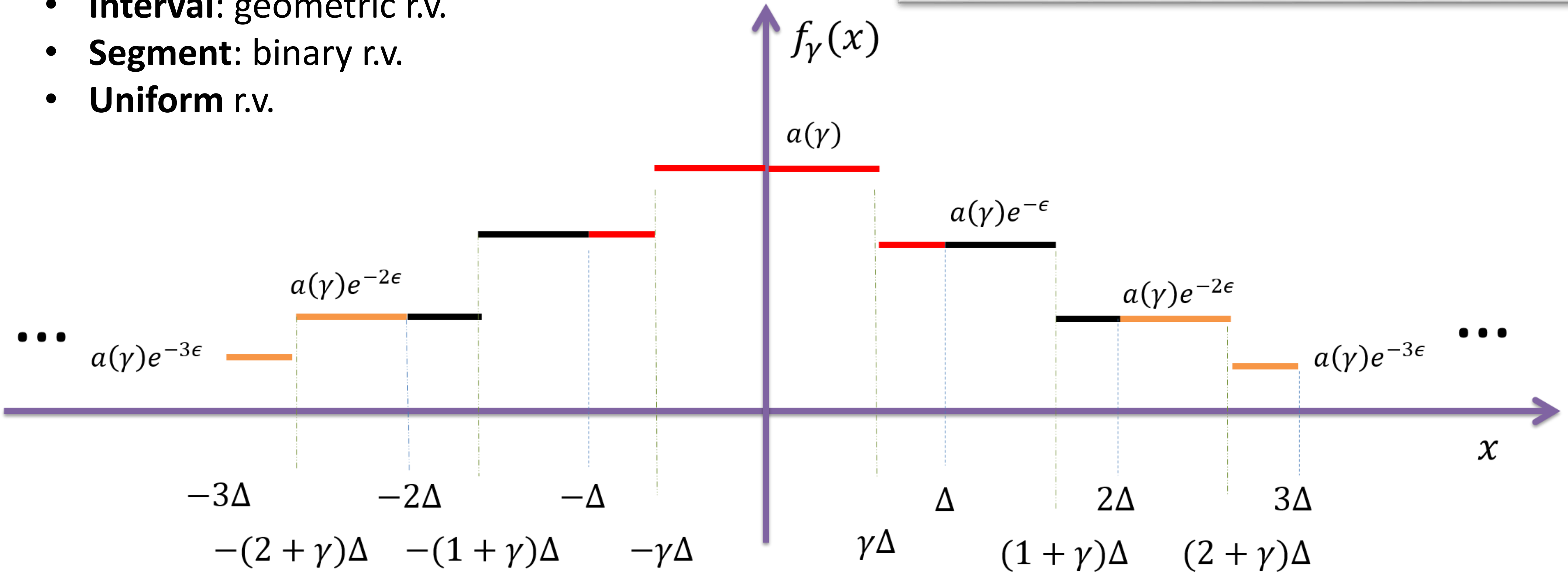


Main Result

$$f_\gamma(x) = \begin{cases} a(\gamma) & x \in [0, \gamma\Delta) \\ e^{-\epsilon} a(\gamma) & x \in [\gamma\Delta, \Delta) \\ e^{-k\epsilon} f_\gamma(x - k\Delta) & x \in [k\Delta, (k+1)\Delta) \\ f_\gamma(-x) & x < 0 \end{cases}$$

R.V. generation

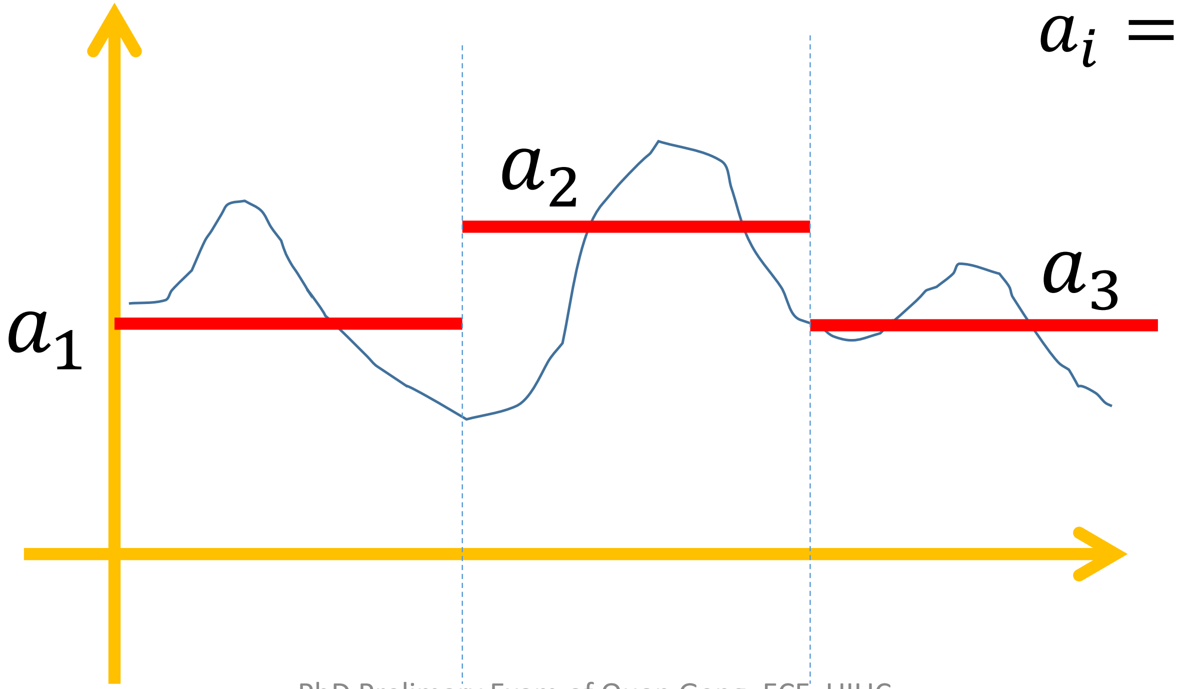
- **Sign**: binary r.v.
- **Interval**: geometric r.v.
- **Segment**: binary r.v.
- **Uniform** r.v.



Proof Ideas

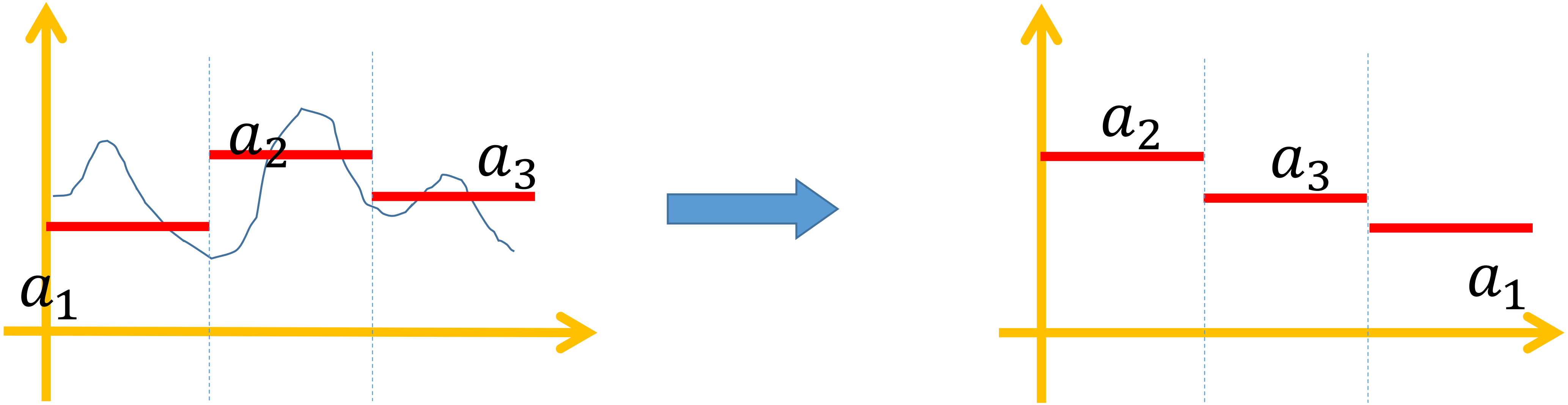
- **Key idea:**
  - Divide each interval $[k\Delta,(k+1)\Delta)$ into i bins
  - Approximate using piecewise constant p.d.f.

$$a_i = \frac{P(interval)}{length(interval)}$$



Proof Ideas

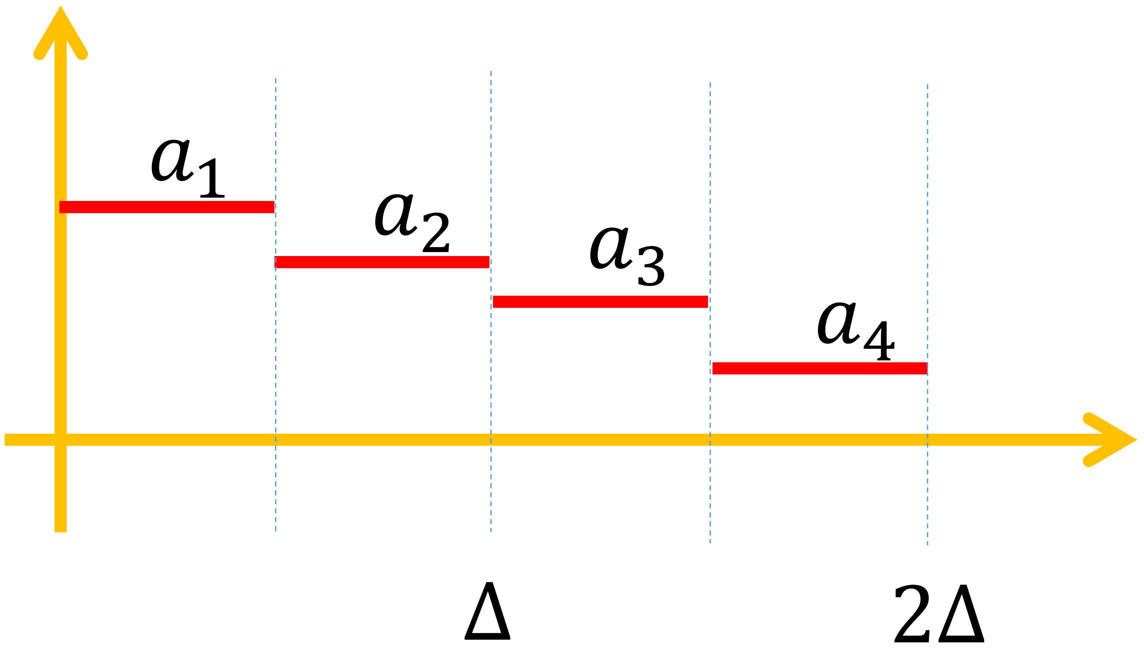
- **p.d.f. should be decreasing**



Proof Ideas

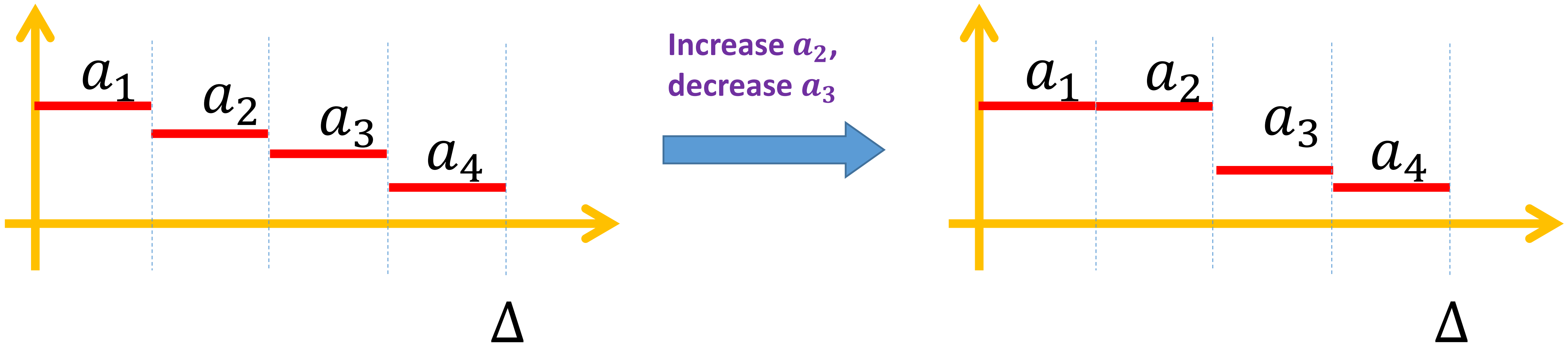
- **p.d.f. should be geometrically decreasing**
  - Divide each interval $[k\Delta, (k+1)\Delta)$ into i bins
  - $\boldsymbol{\frac{a_k}{a_{k+i}} = e^{\epsilon}}$

$\boldsymbol{\frac{a_1}{a_3} = e^{\epsilon}}$, $\boldsymbol{\frac{a_2}{a_4} = e^{\epsilon}}$



Proof Ideas

- The shape of p.d.f. in the first interval $[0, \Delta)$ should be a step function



Application: L(x) = |x|

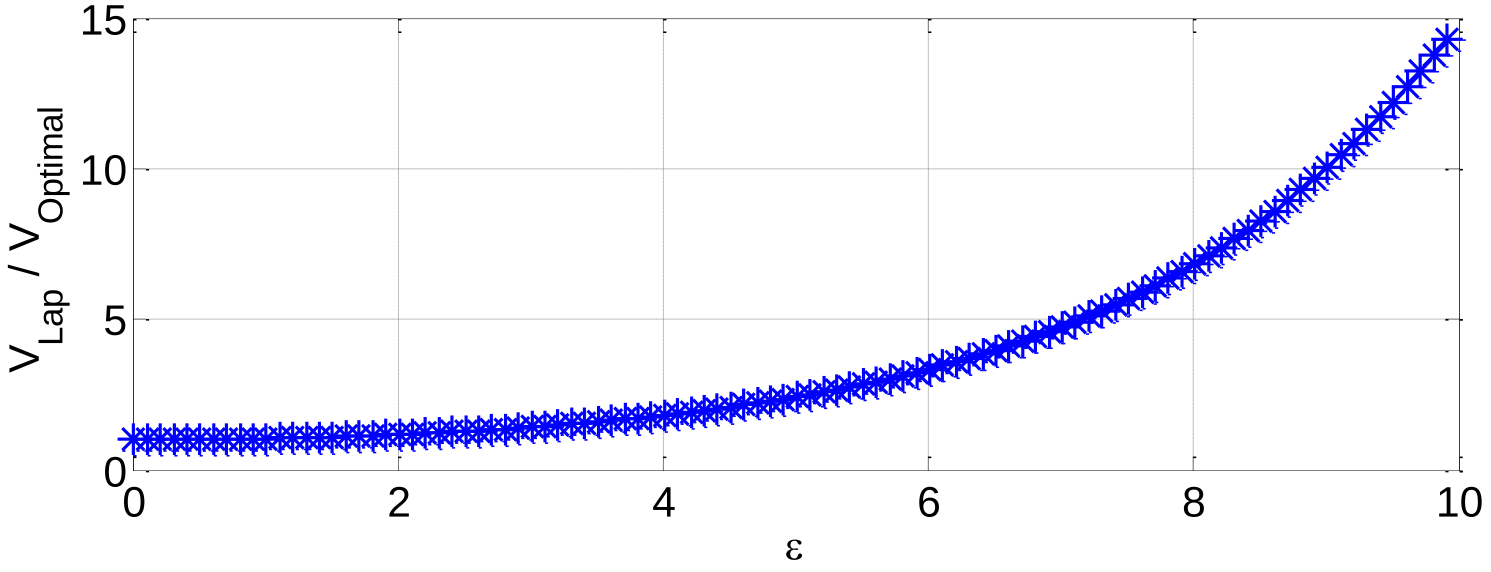
$\gamma^* = \frac{1}{1+e^{\frac{\epsilon}{2}}}$, and the minimum expectation of noise amplitude is

$$V(P_{\gamma^*}) = \Delta \frac{e^{\frac{\epsilon}{2}}}{e^{\epsilon}-1}$$

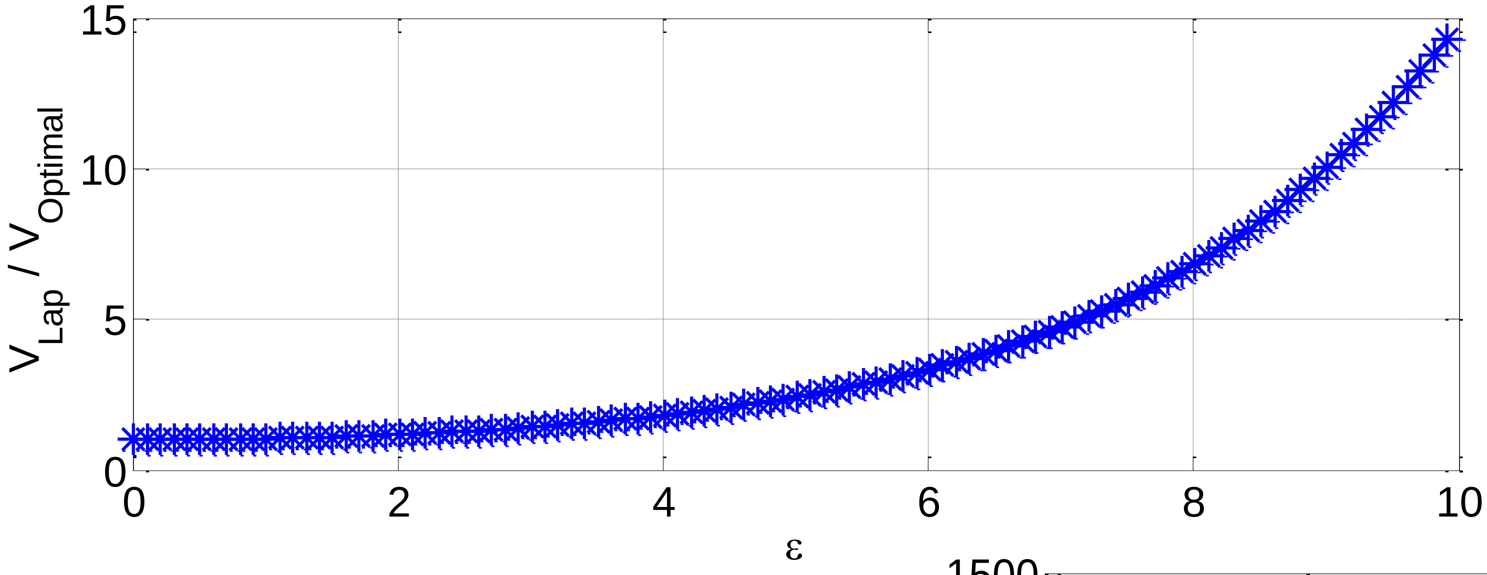
$$V_{Lap} = \frac{\Delta}{\epsilon}$$

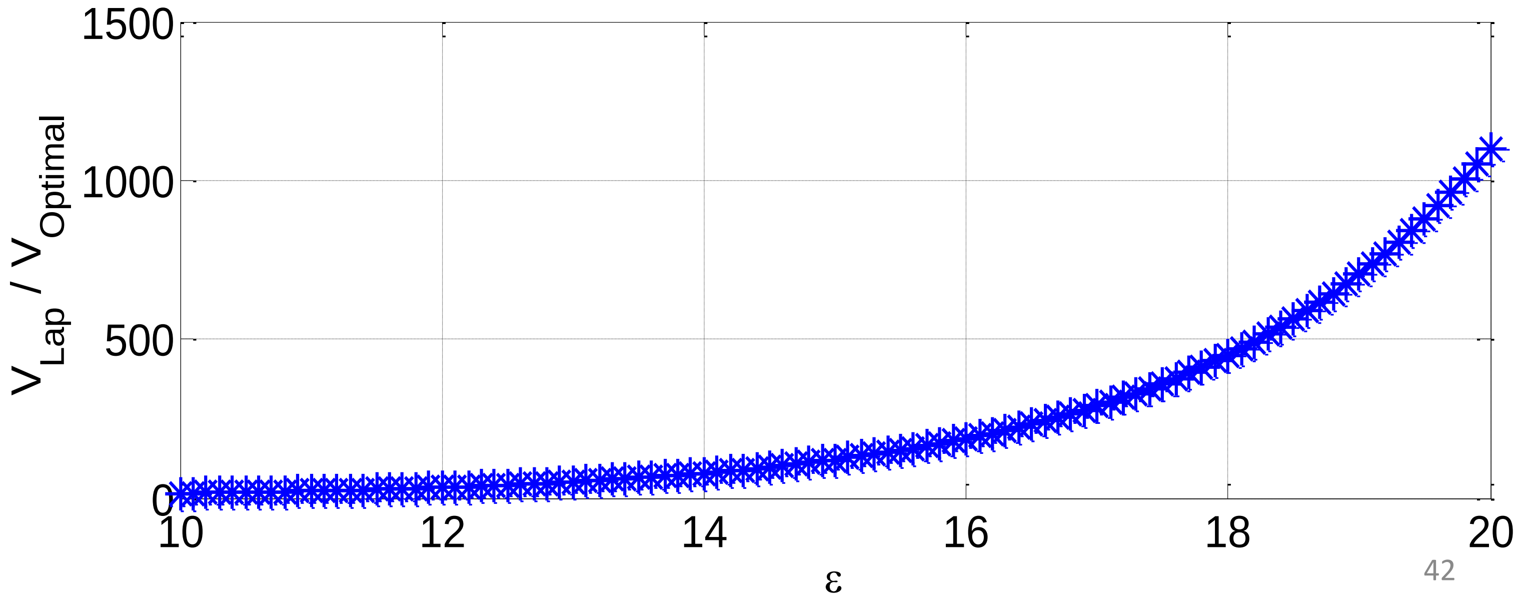
- $\epsilon \to 0$, the additive gap $\to 0$
- $\epsilon \to +\infty$, $V(P_{\gamma^*}) = \Theta(\Delta e^{-\frac{\epsilon}{2}})$

Numeric Comparison with Laplacian Mechanism



Numeric Comparison with Laplacian Mechanism

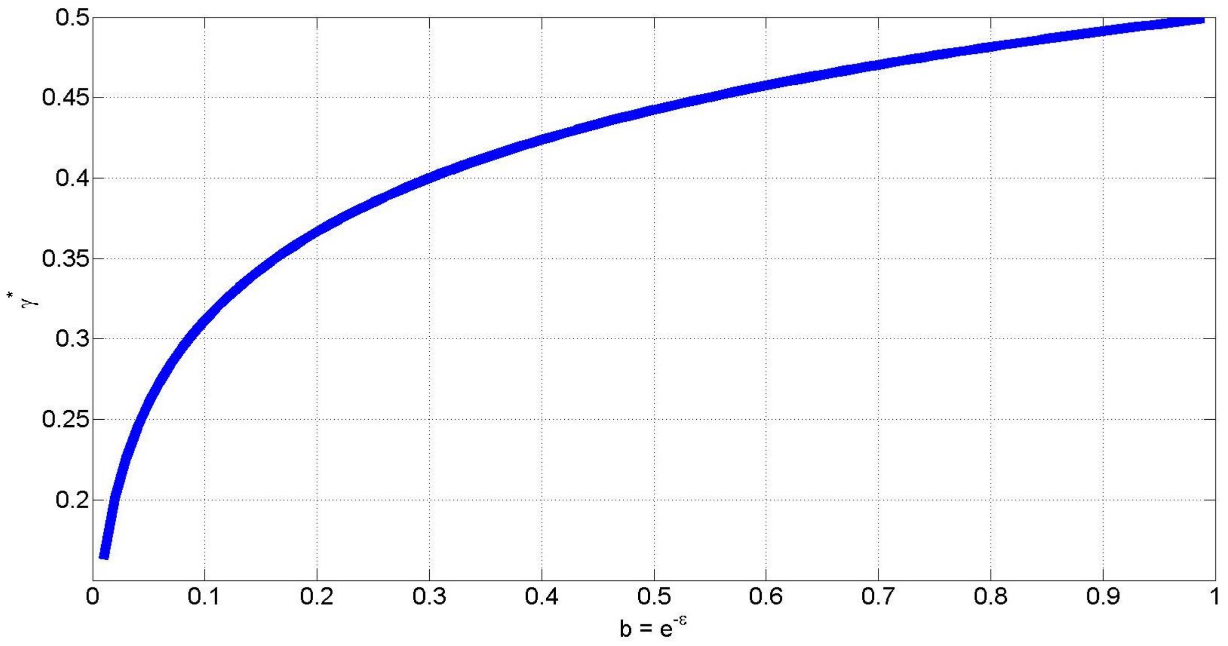




Application: $L(x) = x^2$

- $(b := e^{-\epsilon})$

$$\gamma^* = -\frac{b}{1-b} + \frac{(b - 2b^2 + 2b^4 - b^5)^{1/3}}{2^{1/3}(1-b)^2}$$



Minimum noise power

$$V(\mathcal{P}_{\gamma^*}) = \Delta^2 \frac{2^{-2/3} b^{2/3} (1+b)^{2/3} + b}{(1-b)^2}.$$

Application: $\mathrm{L(x) = x^2}$

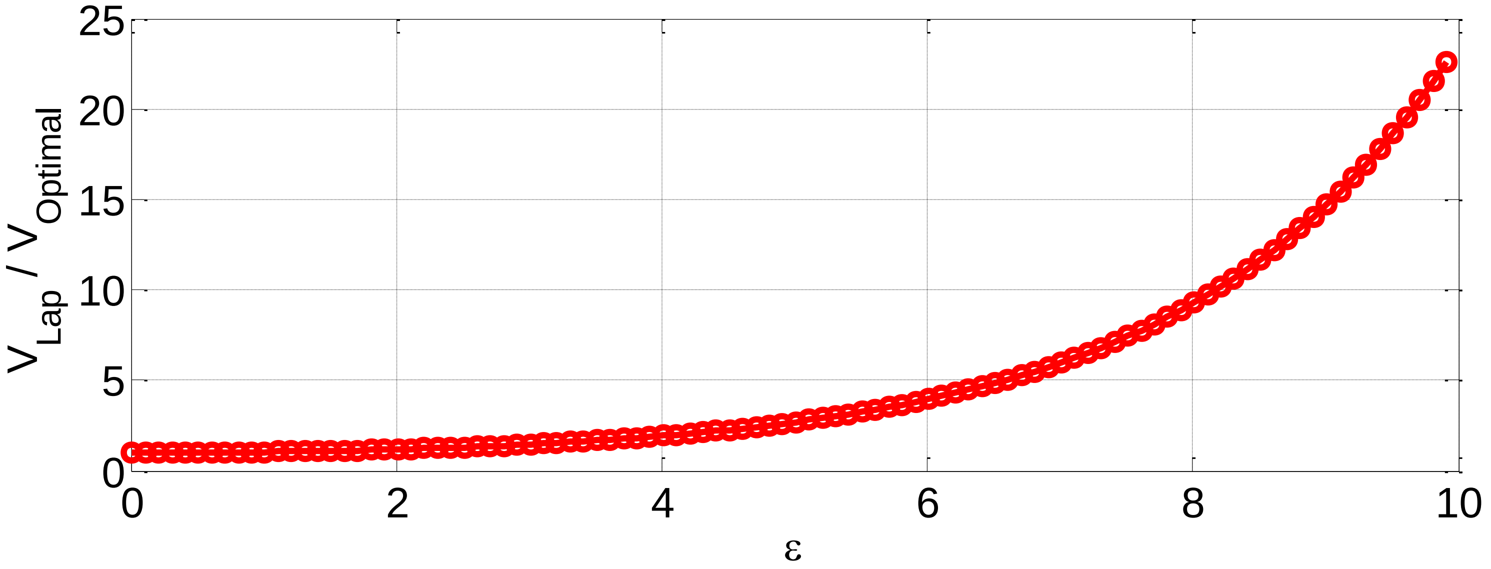
- $(b := e^{-\epsilon})$ The minimum noise power is

$$V(\mathcal{P}_{\gamma^*}) = \Delta^2 \frac{2^{-2/3} b^{2/3} (1+b)^{2/3} + b}{(1-b)^2}.$$

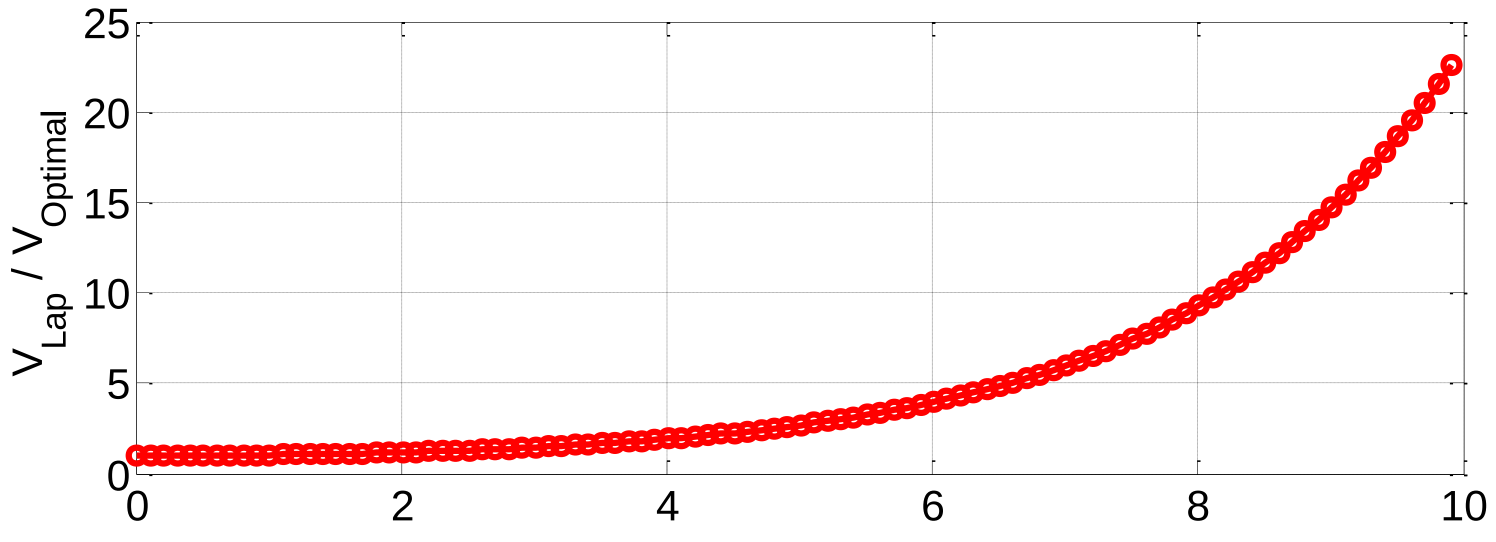
$$V_{Lap} = \frac{2\Delta^2}{\epsilon^2}$$

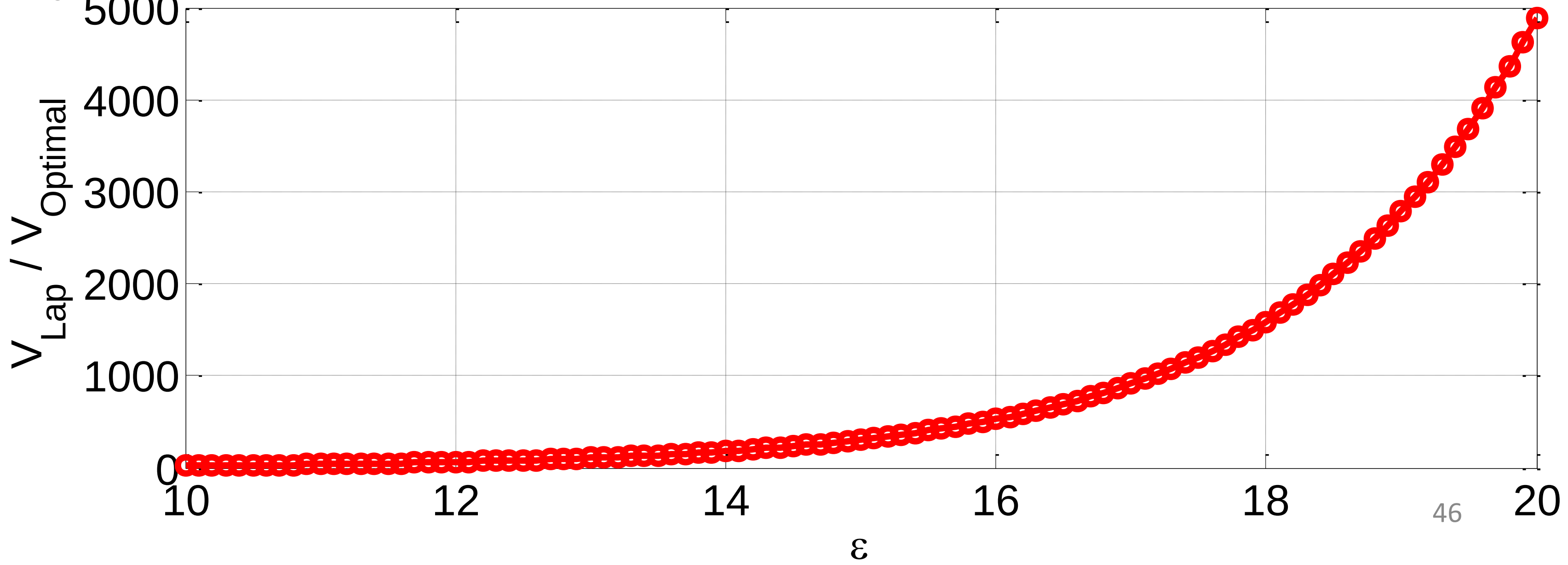
- $\epsilon \to 0$, the additive gap $\leq c\Delta^2$
- $\epsilon \to +\infty$, $V(P_{\gamma^*}) = \Theta(\Delta^2 \, \mathrm{e}^{-\frac{2\epsilon}{3}})$

Numeric Comparison with Laplacian Mechanism



Numeric Comparison with Laplacian Mechanism





Properties of γ^*

- $L(x) = |x|^m$,

$$\gamma^* \to \frac{1}{2}, \; as \; \epsilon \to 0,$$
$$\gamma^* \to 0, \; as \; \epsilon \to +\infty.$$

Also holds for cost functions which are positive linear combinations of momentum functions.

Extension to Discrete Setting

- Query function: $q(D)$ is integer-valued

Extension to Discrete Setting

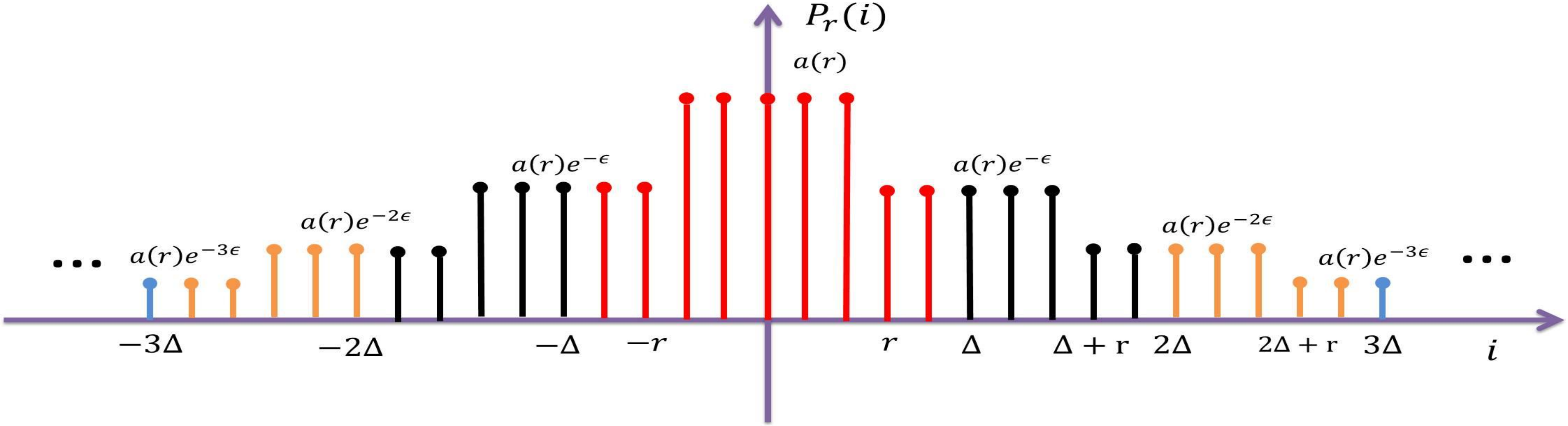
- Query function: $q(D)$ is integer-valued

Adding data-independent noise is optimal

Extension to Discrete Setting

- Query function: $q(D)$ is integer-valued

Adding data-independent noise is optimal



Extension to Abstract Setting

- $K: \boldsymbol{D} \rightarrow \boldsymbol{R}$ (can be arbitrary), with base measure $\boldsymbol{\mu}$.
- Cost function: $\boldsymbol{C}: \boldsymbol{D} \times \boldsymbol{R} \rightarrow [\mathbf{0}, +\infty]$
- Sensitivity

$$\Delta := \max_{r \in R, D_1, D_2 : |D_1 - D_2| \leq 1} |C(D_1, r) - C(D_2, r)|$$

Extension to Abstract Setting

- $K: \boldsymbol{D} \rightarrow \boldsymbol{R}$ (can be arbitrary), with base measure $\boldsymbol{\mu}$.
- Cost function: $\boldsymbol{C}: \boldsymbol{D} \times \boldsymbol{R} \rightarrow [\mathbf{0}, +\infty]$
- Sensitivity

$$\Delta := \max_{r \in R, D_1, D_2 : |D_1 - D_2| \leq 1} |C(D_1, r) - C(D_2, r)|$$

- **Staircase mechanism**:

  Random sampling over the output range with staircase distribution.

Extension to Abstract Setting

- $K: \boldsymbol{D} \rightarrow \boldsymbol{R}$ (can be arbitrary), with base measure $\boldsymbol{\mu}$.
- Cost function: $\boldsymbol{C}: \boldsymbol{D} \times \boldsymbol{R} \rightarrow [\boldsymbol{0}, +\infty]$
- Sensitivity

$$\Delta := \max_{r \in R, D_1, D_2 : |D_1 - D_2| \le 1} |C(D_1, r) - C(D_2, r)|$$

- **Staircase mechanism**:
  Random sampling over the output range with staircase distribution.

- If R is real space, and $C(d, r) = |r - q(d)|$, regular staircase mechanism

Conclusion

- Fundamental tradeoff between privacy and utility in DP
- Staircase Mechanism, optimal mechanism for single real-valued query
  - Huge improvement in low privacy regime
- Extension to discrete setting and abstract setting

Future Work: Multidimensional setting:

- Query output can have multiple components

$$\boldsymbol{q(D) = \left(q_1(D), q_2(D), \dots, q_n(D)\right)}$$

Future Work: Multidimensional setting:

- Query output can have multiple components

$$\boldsymbol{q(D) = \left(q_1(D), q_2(D), \dots, q_n(D)\right)}$$

- If all components are uncorrelated, perturb each component independently to preserve DP.

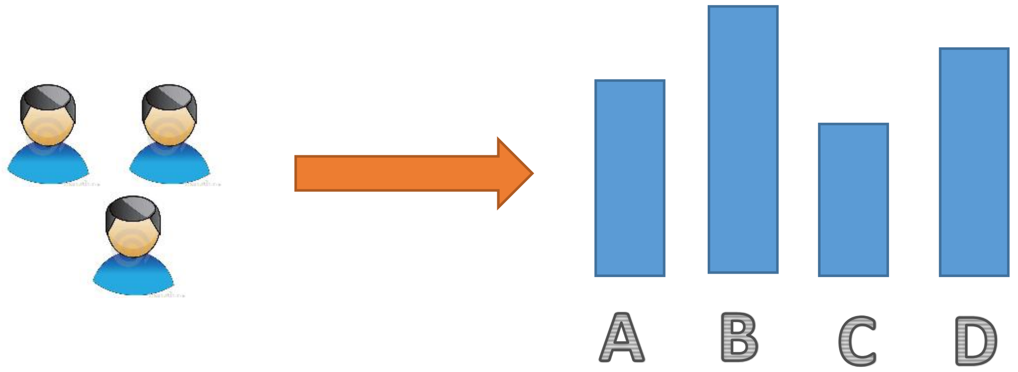
Future Work: Multidimensional setting:

- Query output can have multiple components

$$q(D) = \left(q_1(D), q_2(D), \dots, q_n(D)\right)$$

- For some query, all components are coupled together.

Histogram query:
one user can affect **only one** component



Future Work: Multidimensional setting:

- Query output can have multiple components

$$\boldsymbol{q(D) = \big(q_1(D), q_2(D), \dots, q_n(D)\big)}$$

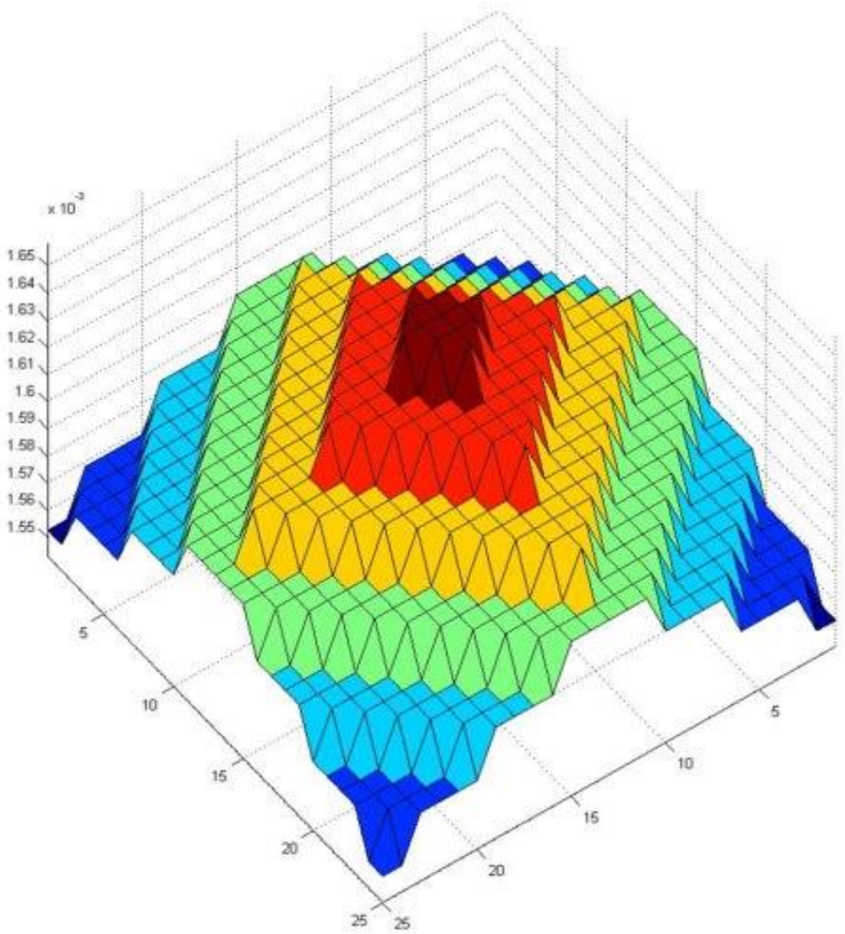
- For some query, all components are coupled together.
- **Global sensitivity**

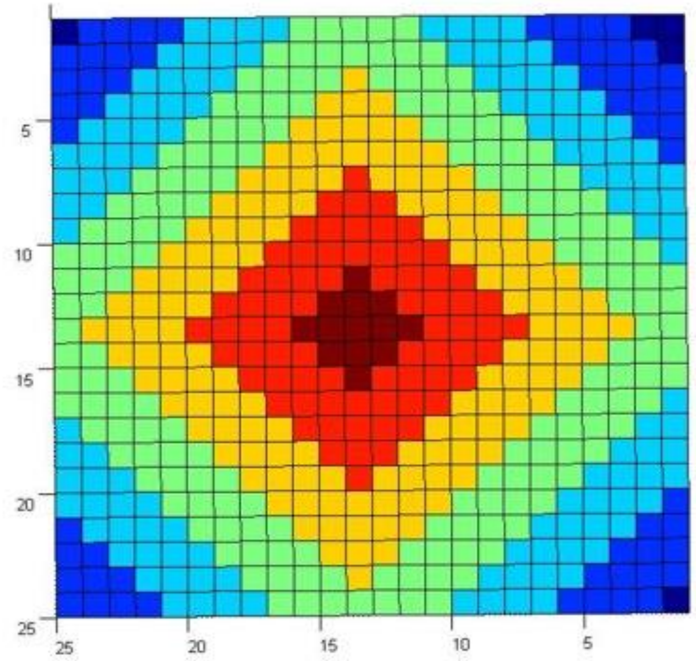
$$\boldsymbol{\Delta} := \max_{\boldsymbol{D_1, D_2\ are\ neighbors}} \boldsymbol{||q(D_1) - q(D_2)||_1}$$

Histogram query: **Δ** = 1

Future Work: Multidimensional setting:

- **Conjecture:** for histogram-like query, optimal noise probability distribution is multidimensional staircase-shaped





Future Work: (ϵ, δ)-differential privacy

- (ϵ, δ)-differential privacy

$$\mathbf{Pr(K(D_1) \in S) \le e^{\epsilon}\, Pr(K(D_2) \in S) + \delta}$$

- The standard approach is to add Gaussian noise.

- What is the **optimal** noise probability distribution in this setting?

Thank you!