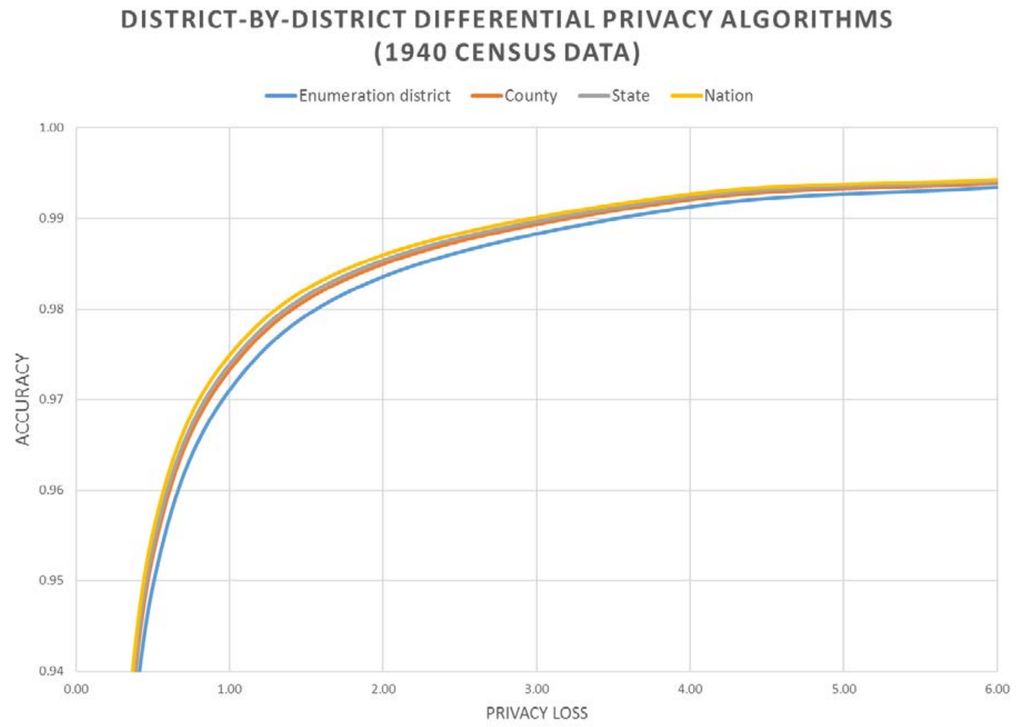
Privacy Amplification

Borja Balle

A Fundamental Trade-off

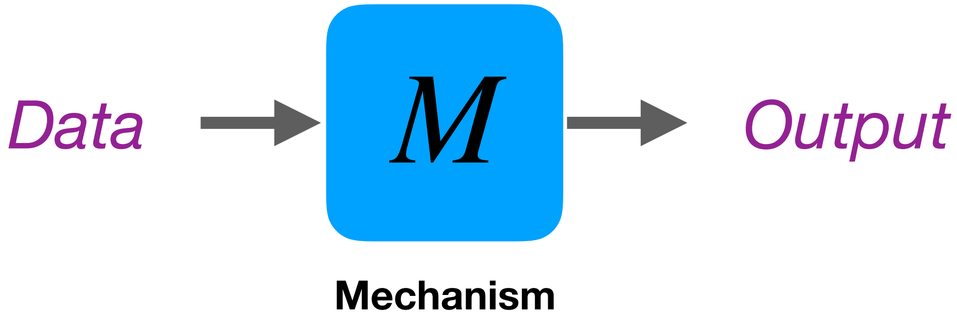
Bridging Theory and Practice

$$O\left(\frac{\sqrt{d\log(1/\delta)}}{n\varepsilon}\right)$$



Plot from J. M. Abowd "Disclosure Avoidance for Block Level Data and Protection of Confidentiality in Public Tabulations" (CSAC Meeting, December 2018)

Privacy Amplification

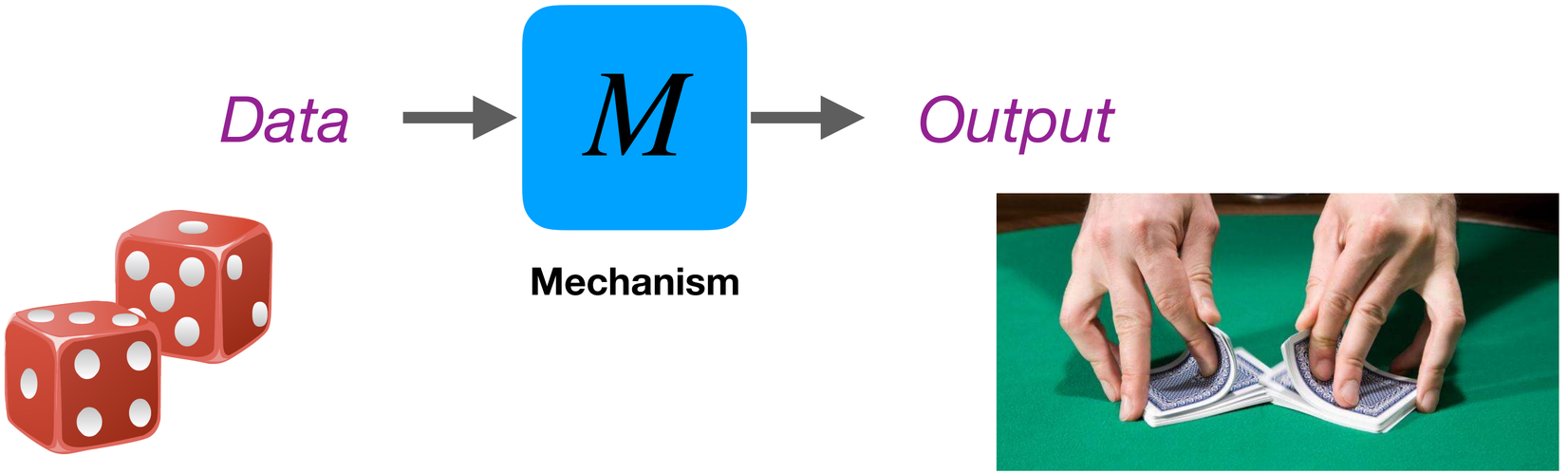


Privacy Amplification

Data → M → *Output*

Mechanism

Privacy Amplification



- Subsampling the input dataset [B, Barthe, Gaboardi NeurIPS'18]
- Shuffling outputs coming from different data records [B, Bell, Gascón, Nissim CRYPTO'19]
- Applying a stochastic post-processing to the output [B, Barthe, Gaboardi, Geumlek arXiv'19]

Motivations

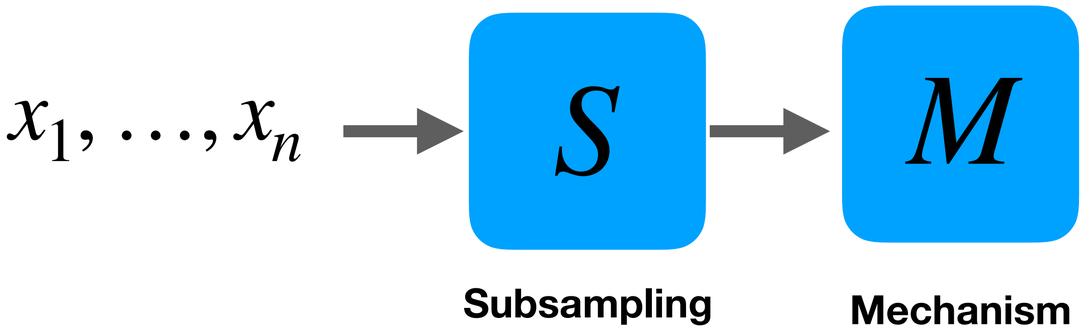
- **New building blocks** for DP mechanisms
- Account for privacy induced by **additional sources of randomness** in existing mechanisms
- **Better utility** through tighter privacy bounds
- Gain a **deeper understanding** of differential privacy
- **Cool, fun** math 😊

In This Talk…

- **The method of overlapping mixtures**
  - Amplification by subsampling
  - Amplification by stochastic post-processing
- **Couplings beyond overlapping mixtures**
  - Amplification by shuffling
  - Amplification by iteration

The Method of Overlapping Mixtures

Amplification by Subsampling

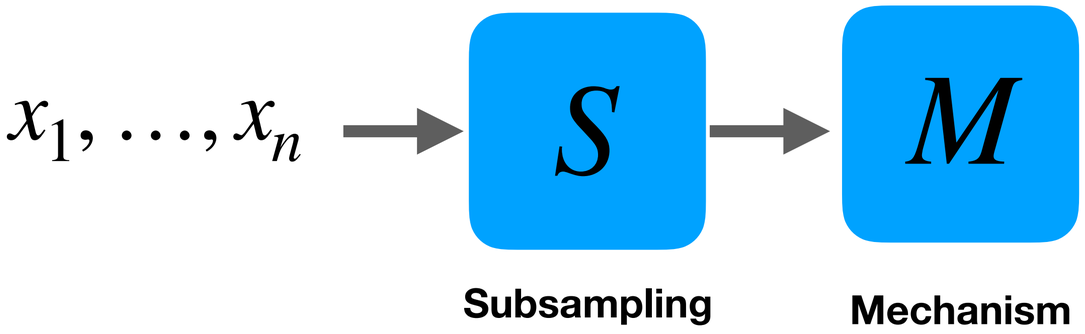


Subsampling

Select a random γ fraction of the original dataset

[CM'06; BKN'10; KLNRS'11; LQS'12; BNS'13; BST'14; BNSV'15]

Amplification by Subsampling



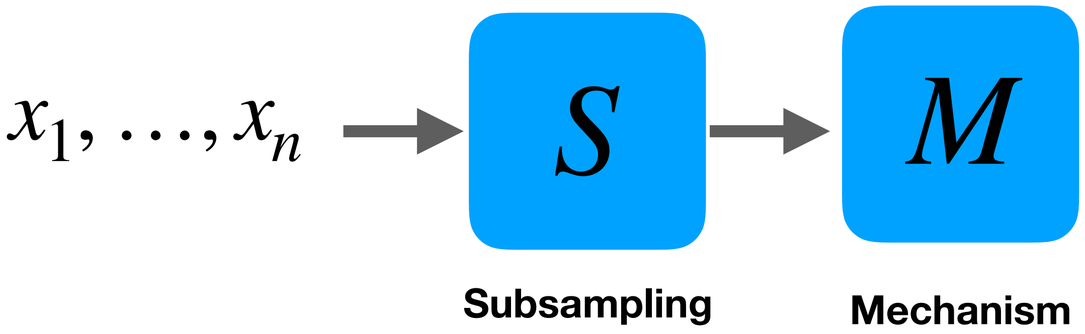
Subsampling

Select a random γ fraction of the original dataset

- Secrecy of the sample: each x_i is used only w.p. γ

[CM'06; BKN'10; KLNRS'11; LQS'12; BNS'13; BST'14; BNSV'15]

Amplification by Subsampling



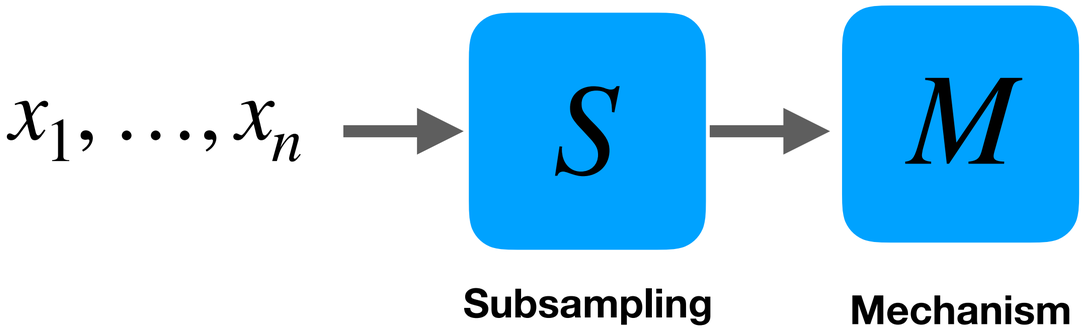
Subsampling

Select a random γ fraction of the original dataset

- Secrecy of the sample: each x_i is used only w.p. γ
- Used in: learning algorithms/theory, stochastic optimization, …

[CM'06; BKN'10; KLNRS'11; LQS'12; BNS'13; BST'14; BNSV'15]

Amplification by Subsampling



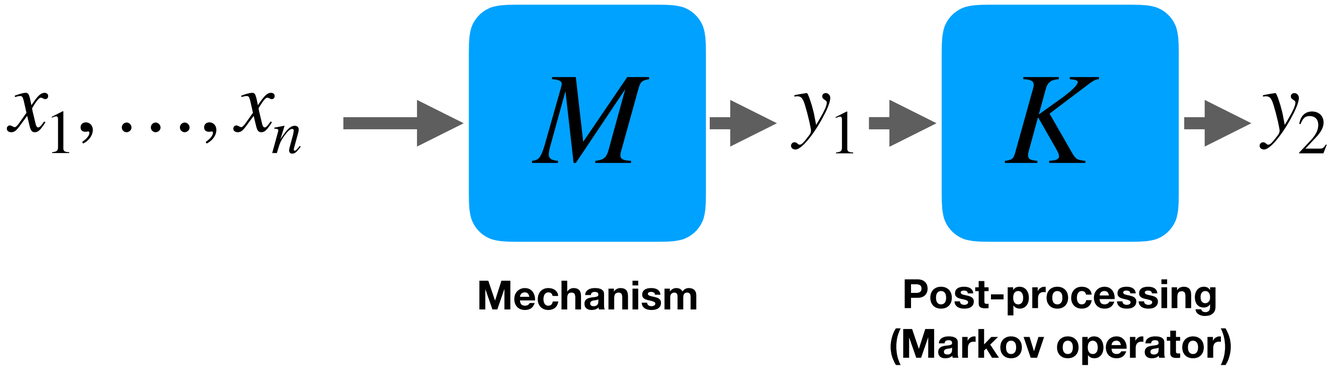
Subsampling

Select a random γ fraction of the original dataset

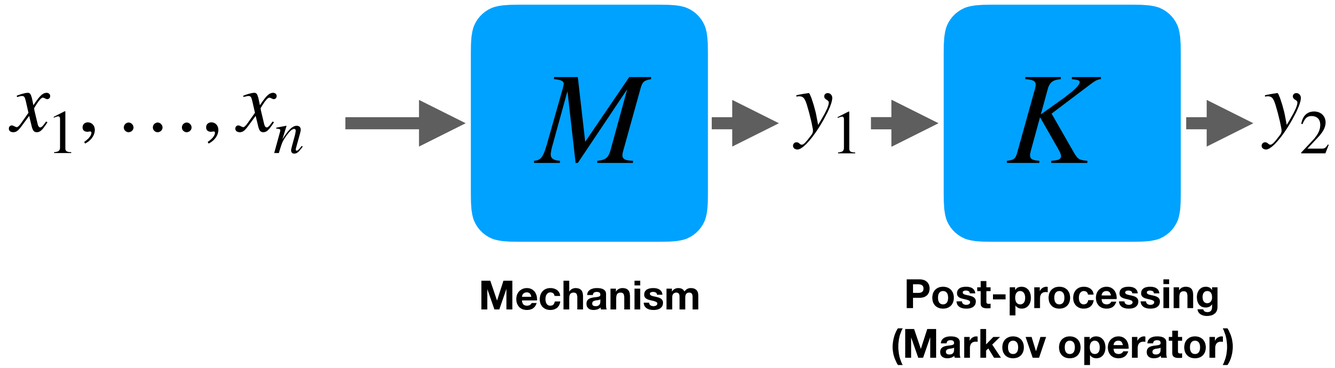
- Secrecy of the sample: each x_i is used only w.p. γ
- Used in: learning algorithms/theory, stochastic optimization, …
- Agnostic to the internals of the mechanism

[CM'06; BKN'10; KLNRS'11; LQS'12; BNS'13; BST'14; BNSV'15]

Amplification by Postprocessing

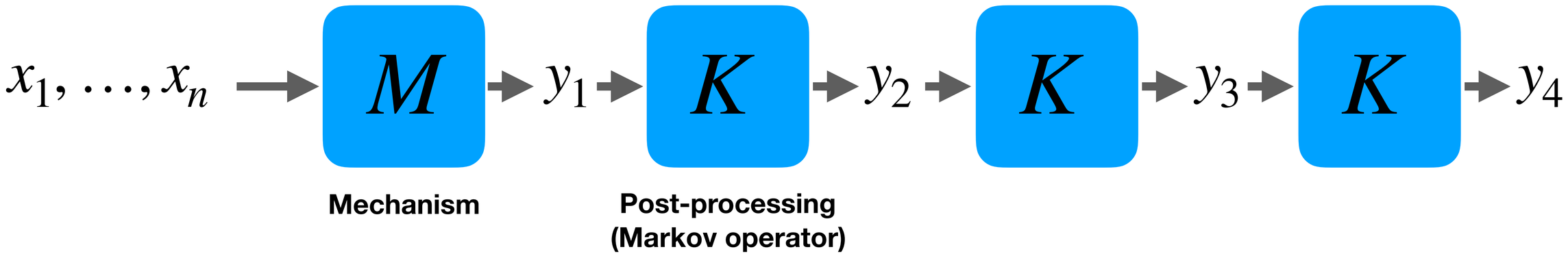


Amplification by Postprocessing



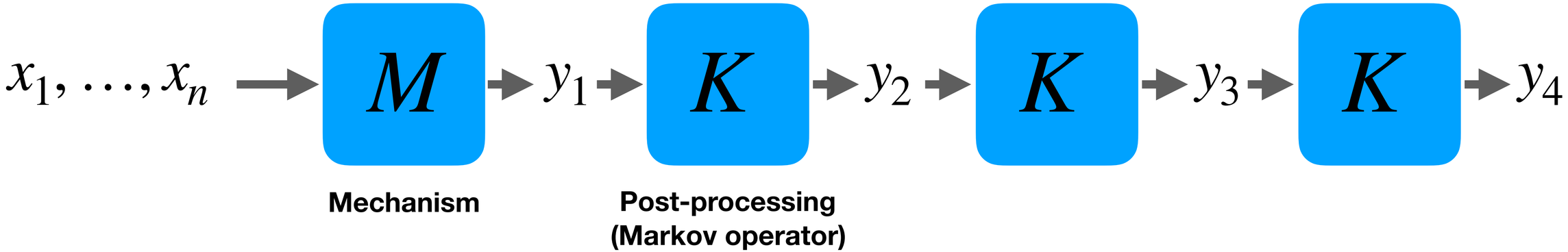
- When is K∘M more private than M?

Amplification by Postprocessing



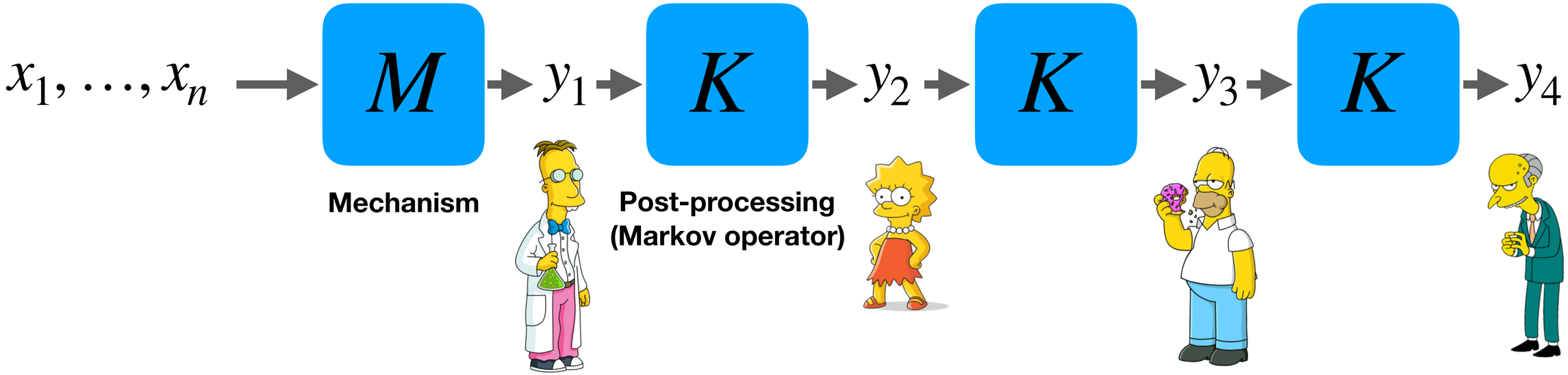
- When is K○M more private than M?

Amplification by Postprocessing



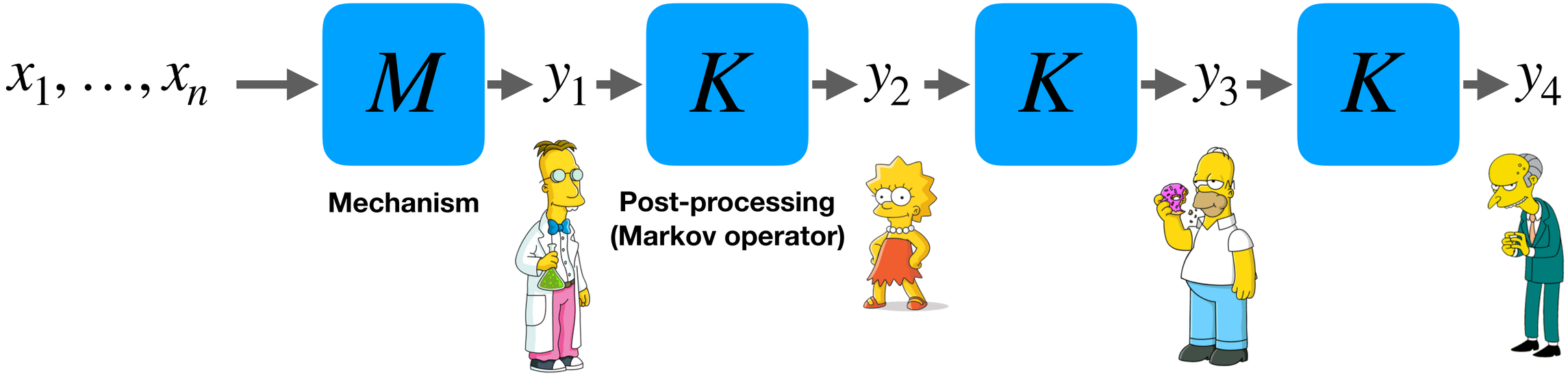
- When is K○M more private than M?
- How does privacy relate to mixing in the Markov chain?

Amplification by Postprocessing



- When is K∘M more private than M?
- How does privacy relate to mixing in the Markov chain?

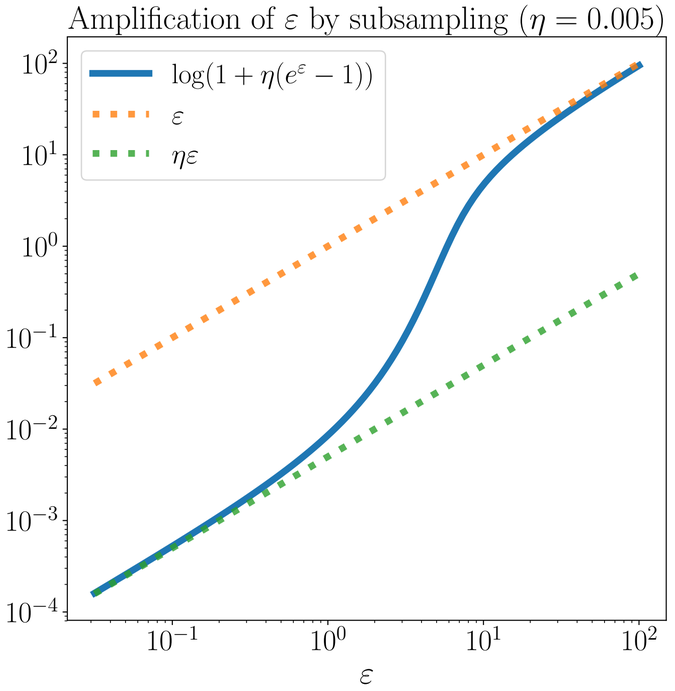
Amplification by Postprocessing



- When is K○M more private than M?
- How does privacy relate to mixing in the Markov chain?
- Starting point for “Hierarchical DP”

Two Amplification Results

- Let M be an (ε,δ)-DP mechanism between "replace one" datasets
- Let ε' = log(1 + γ(e$^{\varepsilon}$-1))
- **Theorem**: If S subsamples a γ fraction w.o.r., then M∘S is (ε',$\gamma\delta$)-DP
- **Theorem**: If K is log(1/(1-γ))-LDP, then K∘M is (ε',$\gamma\delta$e$^{(\varepsilon'-\varepsilon)}$)-DP



DP via Hockey-Stick Divergence

$$\sup_{x \simeq x'} \sup_{E} \left(\Pr[M(x) \in E] - e^{\epsilon} \Pr[M(x') \in E] \right) \leq \delta$$

[BO'13]

DP via Hockey-Stick Divergence

$$\sup_{x \simeq x'} \sup_{E} \left(\Pr[M(x) \in E] - e^{\epsilon} \Pr[M(x') \in E] \right) \leq \delta$$

$$\| $$

$$D_{e^\varepsilon}(M(x) \,|\, M(x')) = \int \left[p_{M(x)}(y) - e^{\epsilon} p_{M(x')}(y) \right]_+ dy$$

[BO'13]

DP via Hockey-Stick Divergence

$$\sup_{x \simeq x'} \sup_{E} \left(\Pr[M(x) \in E] - e^{\epsilon} \Pr[M(x') \in E] \right) \leq \delta$$

$$\Big\Vert$$

$$D_{e^\varepsilon}(M(x) \,|\, M(x')) = \int \Big[p_{M(x)}(y) - e^{\epsilon} p_{M(x')}(y) \Big]_+ dy$$

$$D_{e^\varepsilon}(M(x) \,|\, M(x')) \leq \delta$$

[BO'13]

DP via Hockey-Stick Divergence

$$\sup_{x \simeq x'} \sup_{E} \left(\Pr[M(x) \in E] - e^{\epsilon} \Pr[M(x') \in E] \right) \leq \delta$$

$$\| $$

$$D_{e^\varepsilon}(M(x) \,|\, M(x')) = \int \left[p_{M(x)}(y) - e^{\epsilon} p_{M(x')}(y) \right]_+ dy$$

$$D_{e^\varepsilon}(M(x) \,|\, M(x')) \leq \delta$$

This is an f-divergence, so it satisfies:

- Data processing inequality (ie. postprocessing)
- Joint convexity

[BO'13]

Advanced Joint Convexity of DP

Joint Convexity:

$$\nu = p_1\nu_1 + p_2\nu_2$$
$$\mu = p_1\mu_1 + p_2\mu_2$$

$$\Rightarrow \qquad D_{e^\epsilon}(\mu \,|\, \nu) \le p_1 D_{e^\epsilon}(\mu_1 \,|\, \nu_1) + p_2 D_{e^\epsilon}(\mu_2 \,|\, \nu_2)$$

[BBG'18]

Advanced Joint Convexity of DP

Joint Convexity:

$$\nu = p_1\nu_1 + p_2\nu_2$$
$$\mu = p_1\mu_1 + p_2\mu_2$$
$$\Rightarrow \quad D_{e^\epsilon}(\mu \,|\, \nu) \le p_1 D_{e^\epsilon}(\mu_1 \,|\, \nu_1) + p_2 D_{e^\epsilon}(\mu_2 \,|\, \nu_2)$$

$$\mu_1 = \nu_1 \quad \Rightarrow \quad D_{e^\epsilon}(\mu \,|\, \nu) \le p_2 D_{e^\epsilon}(\mu_2 \,|\, \nu_2)$$

[BBG'18]

Advanced Joint Convexity of DP

Joint Convexity:

$$\begin{aligned}\nu &= p_1\nu_1 + p_2\nu_2\\ \mu &= p_1\mu_1 + p_2\mu_2\end{aligned} \quad \Rightarrow \quad D_{e^\epsilon}(\mu\,|\,\nu) \le p_1 D_{e^\epsilon}(\mu_1\,|\,\nu_1) + p_2 D_{e^\epsilon}(\mu_2\,|\,\nu_2)$$

$$\mu_1 = \nu_1 \quad \Rightarrow \quad D_{e^\epsilon}(\mu\,|\,\nu) \le p_2 D_{e^\epsilon}(\mu_2\,|\,\nu_2)$$

Advanced Joint Convexity: $\tilde{\epsilon} = \log(1 + p_2(e^\epsilon - 1))$

$$\mu_1 = \nu_1 \quad \Rightarrow \quad D_{e^{\tilde{\epsilon}}}(\mu\,|\,\nu) \le p_2 \left(\left(1 - \frac{e^{\tilde{\epsilon}}}{e^\epsilon} \right) D_{e^\epsilon}(\mu_2\,|\,\mu_1) + \frac{e^{\tilde{\epsilon}}}{e^\epsilon} D_{e^\epsilon}(\mu_2\,|\,\nu_2) \right)$$

[BBG'18]

Advanced Joint Convexity of DP

Joint Convexity:

$$\begin{aligned}\nu &= p_1\nu_1 + p_2\nu_2\\ \mu &= p_1\mu_1 + p_2\mu_2\end{aligned} \quad \Rightarrow \quad D_{e^\epsilon}(\mu\,|\,\nu) \le p_1 D_{e^\epsilon}(\mu_1\,|\,\nu_1) + p_2 D_{e^\epsilon}(\mu_2\,|\,\nu_2)$$

$$\mu_1 = \nu_1 \quad \Rightarrow \quad D_{e^\epsilon}(\mu\,|\,\nu) \le p_2 D_{e^\epsilon}(\mu_2\,|\,\nu_2)$$

Advanced Joint Convexity: $\tilde{\epsilon} = \log(1 + p_2(e^\epsilon - 1))$

$$\mu_1 = \nu_1 \quad \Rightarrow \quad D_{e^{\tilde{\epsilon}}}(\mu\,|\,\nu) \le p_2 \left(\left(1 - \frac{e^{\tilde{\epsilon}}}{e^\epsilon}\right) D_{e^\epsilon}(\mu_2\,|\,\mu_1) + \frac{e^{\tilde{\epsilon}}}{e^\epsilon} D_{e^\epsilon}(\mu_2\,|\,\nu_2) \right)$$

[BBG'18]

Overlapping Mixtures in Subsampling

Let M be (ε,δ)-DP and S be subsampling w.o.r. of a γ fraction of the dataset:

$$\Pr[M \circ S(x) \in E] = \Pr_{y \sim S(x)}[M(y) \in E]$$

Overlapping Mixtures in Subsampling

Let M be (ε,δ)-DP and S be subsampling w.o.r. of a γ fraction of the dataset:

$$\Pr[M \circ S(x) \in E] = \Pr_{y \sim S(x)}[M(y) \in E]$$

Let x and x' differ in one record:

$$M \circ S(x): \quad \Pr[x_n \notin y] \Pr[M(y) \in E \,|\, x_n \notin y] + \Pr[x_n \in y] \Pr[M(y) \in E \,|\, x_n \in y]$$

$$M \circ S'(x): \quad \Pr[x'_n \notin y] \Pr[M(y) \in E \,|\, x'_n \notin y] + \Pr[x'_n \in y] \Pr[M(y) \in E \,|\, x'_n \in y]$$

Overlapping Mixtures in Subsampling

Let M be (ε,δ)-DP and S be subsampling w.o.r. of a γ fraction of the dataset:

$$\Pr[M \circ S(x) \in E] = \Pr_{y \sim S(x)}[M(y) \in E]$$

Let x and x' differ in one record:

μ_1 μ_2

$$M \circ S(x): \quad \Pr[x_n \notin y] \Pr[M(y) \in E \mid x_n \notin y] + \Pr[x_n \in y] \Pr[M(y) \in E \mid x_n \in y]$$

$p_1 = 1 - \gamma$ $p_2 = \gamma$

$$M \circ S'(x): \quad \Pr[x'_n \notin y] \Pr[M(y) \in E \mid x'_n \notin y] + \Pr[x'_n \in y] \Pr[M(y) \in E \mid x'_n \in y]$$

ν_1 ν_2

Overlapping Mixtures in Subsampling

Let M be (ε,δ)-DP and S be subsampling w.o.r. of a γ fraction of the dataset:

$$\Pr[M \circ S(x) \in E] = \Pr_{y \sim S(x)}[M(y) \in E]$$

Let x and x' differ in one record:

$$M \circ S(x): \quad \Pr[x_n \notin y]\,\underbrace{\Pr[M(y) \in E \mid x_n \notin y]}_{\mu_1} + \Pr[x_n \in y]\,\underbrace{\Pr[M(y) \in E \mid x_n \in y]}_{\mu_2}$$

$p_1 = 1 - \gamma$ $\qquad$ $p_2 = \gamma$

$$M \circ S'(x): \quad \Pr[x'_n \notin y]\,\underbrace{\Pr[M(y) \in E \mid x'_n \notin y]}_{\nu_1} + \Pr[x'_n \in y]\,\underbrace{\Pr[M(y) \in E \mid x'_n \in y]}_{\nu_2}$$

Overlapping Mixtures in Subsampling

Let M be (ε,δ)-DP and S be subsampling w.o.r. of a γ fraction of the dataset:

$$\Pr[M \circ S(x) \in E] = \Pr_{y \sim S(x)}[M(y) \in E]$$

Let x and x' differ in one record:

$$M \circ S(x): \quad \Pr[x_n \notin y]\,\underbrace{\Pr[M(y) \in E \mid x_n \notin y]}_{\mu_1} + \Pr[x_n \in y]\,\underbrace{\Pr[M(y) \in E \mid x_n \in y]}_{\mu_2}$$

$$p_1 = 1 - \gamma \qquad\qquad p_2 = \gamma$$

$$M \circ S'(x): \quad \Pr[x'_n \notin y]\,\underbrace{\Pr[M(y) \in E \mid x'_n \notin y]}_{\nu_1} + \Pr[x'_n \in y]\,\underbrace{\Pr[M(y) \in E \mid x'_n \in y]}_{\nu_2}$$

Bound the divergences:

$$y_2 \sim S_{\gamma n-1}(x \backslash x_n) \cup \{x_n\} \qquad y_1 \sim S_{\gamma n}(x \backslash x_n) \qquad y_2 \simeq y_1 \Rightarrow D_{e^\epsilon}(\mu_2 \mid \mu_1) \leq \delta$$

Coupling

Joint Convexity

Overlapping Mixtures in Subsampling

Let M be (ε,δ)-DP and S be subsampling w.o.r. of a γ fraction of the dataset:

$$\Pr[M \circ S(x) \in E] = \Pr_{y \sim S(x)}[M(y) \in E]$$

Let x and x' differ in one record:

$$M \circ S(x): \quad \Pr[x_n \notin y]\,\underbrace{\Pr[M(y) \in E \mid x_n \notin y]}_{\mu_1} + \Pr[x_n \in y]\,\underbrace{\Pr[M(y) \in E \mid x_n \in y]}_{\mu_2}$$

$$p_1 = 1-\gamma \qquad\qquad p_2 = \gamma$$

$$M \circ S'(x): \quad \Pr[x'_n \notin y]\,\underbrace{\Pr[M(y) \in E \mid x'_n \notin y]}_{\nu_1} + \Pr[x'_n \in y]\,\underbrace{\Pr[M(y) \in E \mid x'_n \in y]}_{\nu_2}$$

Bound the divergences:

$$y_2 \sim S_{\gamma n-1}(x \backslash x_n) \cup \{x_n\} \qquad y_1 \sim S_{\gamma n}(x \backslash x_n) \qquad y_2 \simeq y_1 \quad \text{(Coupling)} \quad \Rightarrow \quad D_{e^\epsilon}(\mu_2 \mid \mu_1) \le \delta$$

$$y_2 \sim S_{\gamma n-1}(x \backslash x_n) \cup \{x_n\} \qquad y'_2 \sim S_{\gamma n-1}(x' \backslash x'_n) \cup \{x'_n\} \qquad y_2 \simeq y'_2 \quad \text{(Coupling)} \quad \Rightarrow \quad D_{e^\epsilon}(\mu_2 \mid \nu_2) \le \delta \quad \text{(Joint Convexity)}$$

Overlapping Mixtures in Postprocessing

Let K be log(1/(1-γ))-LDP. For any ω in the image of K: *[DLM'03]*

$$\Pr[K \circ M(x) \in E] = (1-\gamma)\omega(E) + \gamma \Pr[\tilde{K} \circ M(x) \in E] \quad \text{with} \quad \tilde{K} = \frac{K - (1-\gamma)\omega}{\gamma}$$

[BBGG'19]

Overlapping Mixtures in Postprocessing

Let K be log(1/(1-γ))-LDP. For any ω in the image of K: *[DLM'03]*

$$\Pr[K \circ M(x) \in E] = (1-\gamma)\omega(E) + \gamma \Pr[\tilde{K} \circ M(x) \in E] \quad \text{with} \quad \tilde{K} = \frac{K - (1-\gamma)\omega}{\gamma}$$

Applying advanced joint convexity:

$$D_{e^{\tilde{\epsilon}}}(K \circ M(x) \,|\, K \circ M(x')) \leq \gamma \left(\left(1 - \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}} \right) D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \omega) + \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}} D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \tilde{K} \circ M(x')) \right)$$

[BBGG'19]

Overlapping Mixtures in Postprocessing

Let K be log(1/(1-γ))-LDP. For any ω in the image of K: *[DLM'03]*

$$\Pr[K \circ M(x) \in E] = (1-\gamma)\omega(E) + \gamma \Pr[\tilde{K} \circ M(x) \in E] \quad \text{with} \quad \tilde{K} = \frac{K - (1-\gamma)\omega}{\gamma}$$

Applying advanced joint convexity:

$$D_{e^{\tilde{\epsilon}}}(K \circ M(x) \,|\, K \circ M(x')) \leq \gamma \left(\left(1 - \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}}\right) D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \omega) + \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}} \underbrace{D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \tilde{K} \circ M(x'))}_{\leq \delta} \right)$$

[BBGG'19]

Overlapping Mixtures in Postprocessing

Let K be log(1/(1-γ))-LDP. For any ω in the image of K: [DLM'03]

$$\Pr[K \circ M(x) \in E] = (1-\gamma)\omega(E) + \gamma \Pr[\tilde{K} \circ M(x) \in E] \quad \text{with} \quad \tilde{K} = \frac{K - (1-\gamma)\omega}{\gamma}$$

Applying advanced joint convexity:

$$D_{e^{\tilde{\epsilon}}}(K \circ M(x) \,|\, K \circ M(x')) \leq \gamma \left(\left(1 - \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}}\right) D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \omega) + \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}} \underbrace{D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \tilde{K} \circ M(x'))}_{\leq \delta} \right)$$

Taking ω = K∘M(x):

$$\tilde{K} \circ M(x) = \frac{K \circ M(x) - (1-\gamma) K \circ M(x)}{\gamma} = K \circ M(x)$$

[BBGG'19]

Overlapping Mixtures in Postprocessing

Let K be log(1/(1-γ))-LDP. For any ω in the image of K: [DLM'03]

$$\Pr[K \circ M(x) \in E] = (1-\gamma)\omega(E) + \gamma \Pr[\tilde{K} \circ M(x) \in E] \quad \text{with} \quad \tilde{K} = \frac{K - (1-\gamma)\omega}{\gamma}$$

Applying advanced joint convexity:

$$D_{e^{\tilde{\epsilon}}}(K \circ M(x) \,|\, K \circ M(x')) \leq \gamma \left(\left(1 - \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}}\right) \underbrace{D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \omega)}_{=0} + \frac{e^{\tilde{\epsilon}}}{e^{\epsilon}} \underbrace{D_{e^{\epsilon}}(\tilde{K} \circ M(x) \,|\, \tilde{K} \circ M(x'))}_{\leq \delta} \right)$$

Taking ω = K∘M(x):

$$\tilde{K} \circ M(x) = \frac{K \circ M(x) - (1-\gamma) K \circ M(x)}{\gamma} = K \circ M(x)$$

[BBGG'19]

Further Results

Subsampling	$\simeq_Y$	$\simeq_X$	η	δ'	Theorem
Poisson(γ)	R	R	γ	$\gamma\delta$	13
WOR(n,m)	S	S	$\frac{m}{n}$	$\frac{m}{n}\delta$	14
WR(n,m)	S	S	$1-\left(1-\frac{1}{n}\right)^m$	$\sum_{k=1}^{m}\binom{m}{k}\left(\frac{1}{n}\right)^k\left(1-\frac{1}{n}\right)^{m-k}\delta_k$	15
WR(n,m)	S	R	$1-\left(1-\frac{1}{n}\right)^m$	$\sum_{k=1}^{m}\binom{m}{k}\left(\frac{1}{n}\right)^k\left(1-\frac{1}{n}\right)^{m-k}\delta_k$	16

TABLE 1. Summary of privacy amplification bounds. Amplification parameter η: $e^{\varepsilon'} = 1+\eta(e^{\varepsilon}-1)$. Types of subsampling: without replacement (WOR) and with replacement (WR). Neighbouring relations: remove/add-one (R) and substitute one (S).

Amplification by subsampling in Rényi DP

[WBK'19; ZW'19]

[BBG'18]

Theorem 1. *Let M be an (ε,δ)-DP mechanism. For a given Markov operator K, the post-processed mechanism $K\circ M$ satisfies:*

(1) (ε,δ')-DP with $\delta'=\gamma\delta$ if K is γ-Dobrushin,

(2) (ε,δ')-DP with $\delta'=\gamma\delta$ if K is $(\gamma,\tilde{\varepsilon})$-Dobrushin with[3] $\tilde{\varepsilon}=\log(1+\frac{e^{\varepsilon}-1}{\delta})$,

(3) (ε',δ')-DP with $\varepsilon'=\log(1+\gamma(e^{\varepsilon}-1))$ and $\delta'=\gamma(1-e^{\varepsilon'-\varepsilon}(1-\delta))$ if K is γ-Doeblin,

(4) (ε',δ')-DP with $\varepsilon'=\log(1+\gamma(e^{\varepsilon}-1))$ and $\delta'=\gamma\delta e^{\varepsilon'-\varepsilon}$ if K is γ-ultra-mixing.

Mixing Condition	Local DP Condition
γ-Dobrushin	$(0,\gamma)$-LDP
(γ,ε)-Dobrushin	(ε,γ)-LDP
γ-Doeblin	Blanket condition[4]
γ-ultra-mixing	$(\log\frac{1}{1-\gamma},0)$-LDP

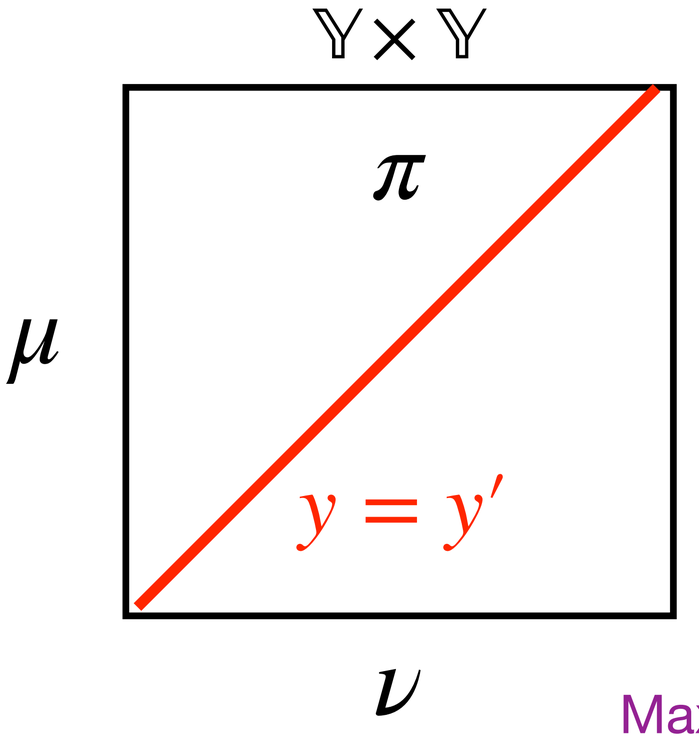
[BBGG'19]

Overlapping Mixtures as Couplings

$$TV(\mu, \nu) = \inf_{\pi \in C(\mu,\nu)} \Pr_{(Y,Y') \sim \pi} [Y \neq Y'] = 1 - \int \min\{p_\mu(y), p_\nu(y)\} dy = \gamma$$

Overlapping Mixtures as Couplings

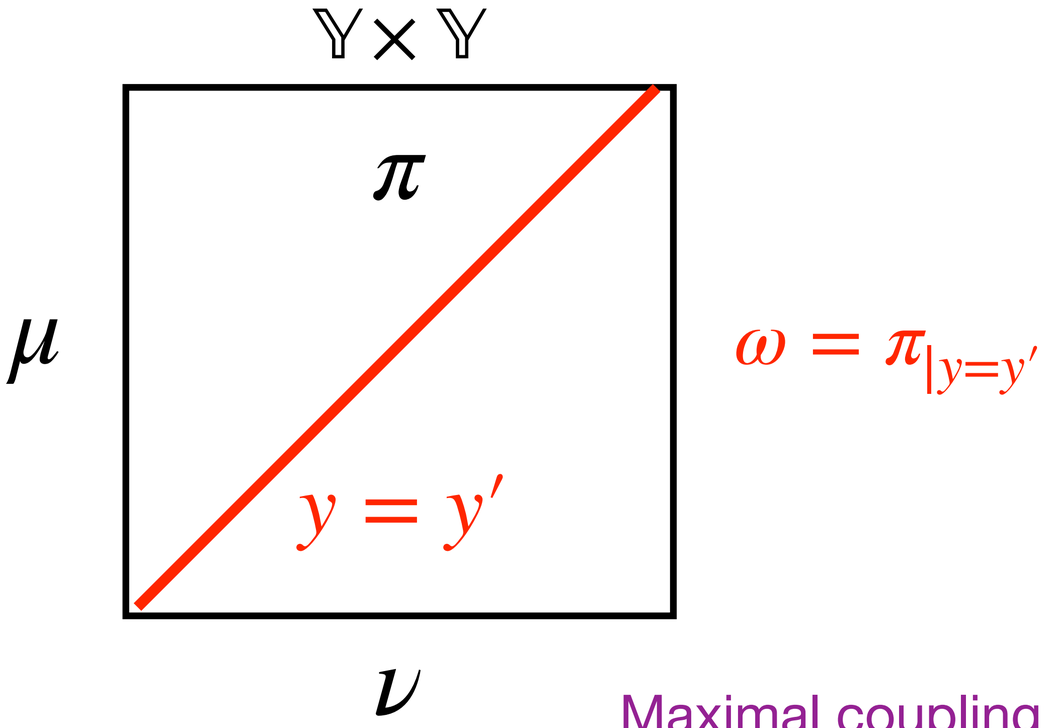
$$TV(\mu,\nu) = \inf_{\pi \in C(\mu,\nu)} \Pr_{(Y,Y')\sim\pi}[Y \neq Y'] = 1 - \int \min\{p_\mu(y), p_\nu(y)\}dy = \gamma$$



Maximal coupling: put as much mass as possible on the diagonal!

Overlapping Mixtures as Couplings

$$TV(\mu,\nu) = \inf_{\pi \in C(\mu,\nu)} \Pr_{(Y,Y')\sim\pi}[Y \neq Y'] = 1 - \int \min\{p_\mu(y), p_\nu(y)\}dy = \gamma$$



$$\omega = \pi_{|y=y'}$$

$$\mu = (1-\gamma)\omega + \gamma\mu_2$$

$$\nu = (1-\gamma)\omega + \gamma\nu_2$$

Maximal coupling: put as much mass as possible on the diagonal!

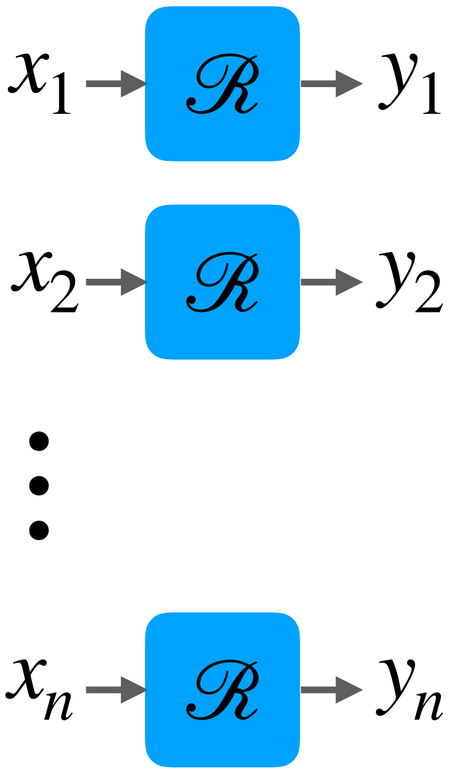
Couplings Beyond Overlapping Mixtures

Other Coupling Strategies

- The maximal coupling leads to two components:
  - One component does not depend on the “data that changed”
  - The remaining components have disjoint support: $\mu_2 \perp \nu_2$
- More than two components might be necessary
  - Amplification by shuffling: as many components as individuals
- In some applications disjoint support is not the right condition
  - Amplification by iteration: keep all mass close to the diagonal

The Shuffle Model

$\mathscr{R} : \mathbb{X} \to \mathbb{Y}$

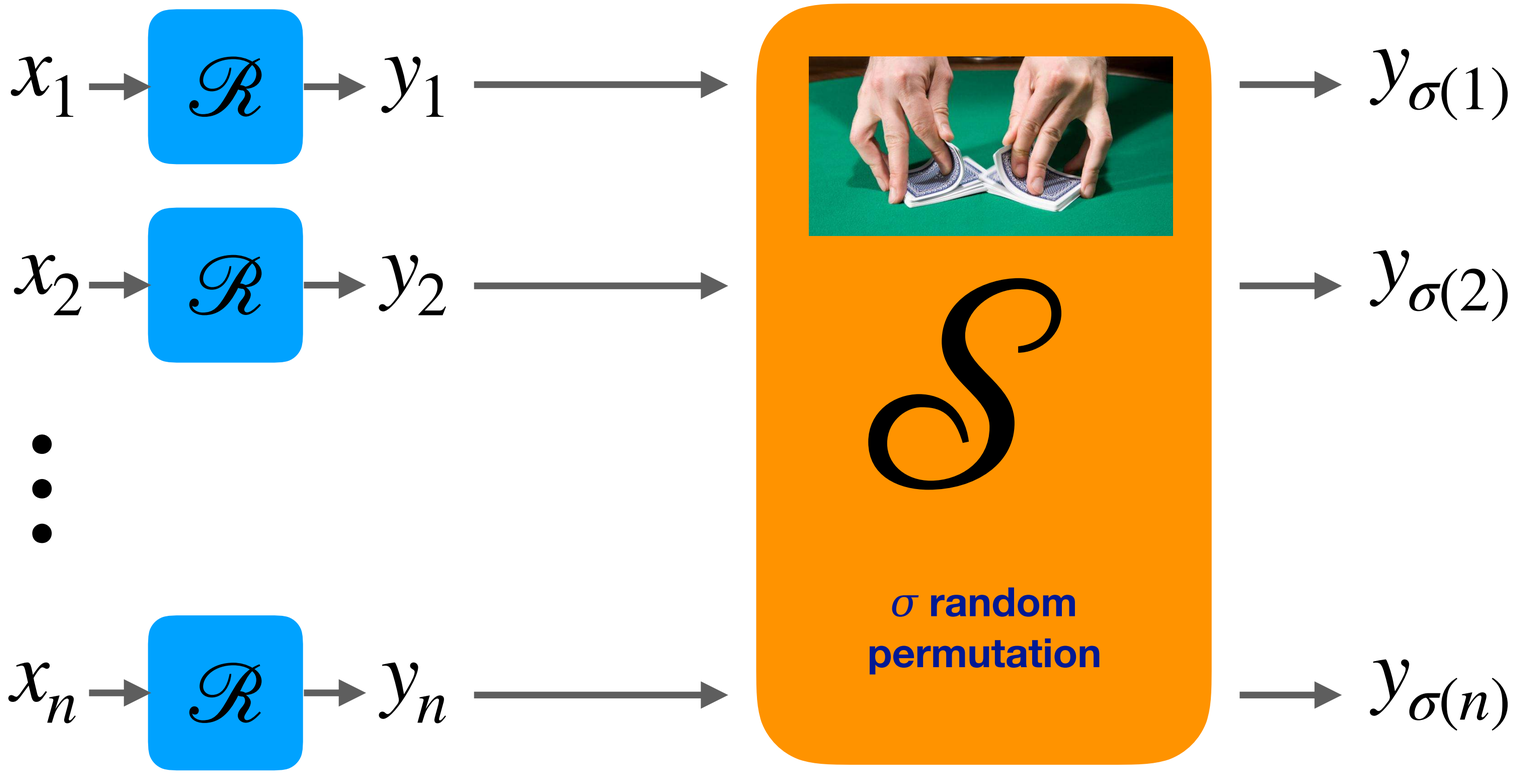


Local Randomizer

[BEMMRLRKTS17; EFMRTT19; CSUZZ19]

The Shuffle Model

$\mathscr{R} : \mathbb{X} \to \mathbb{Y}$ $\mathscr{S} : \mathbb{Y}^n \to \mathbb{Y}^n$



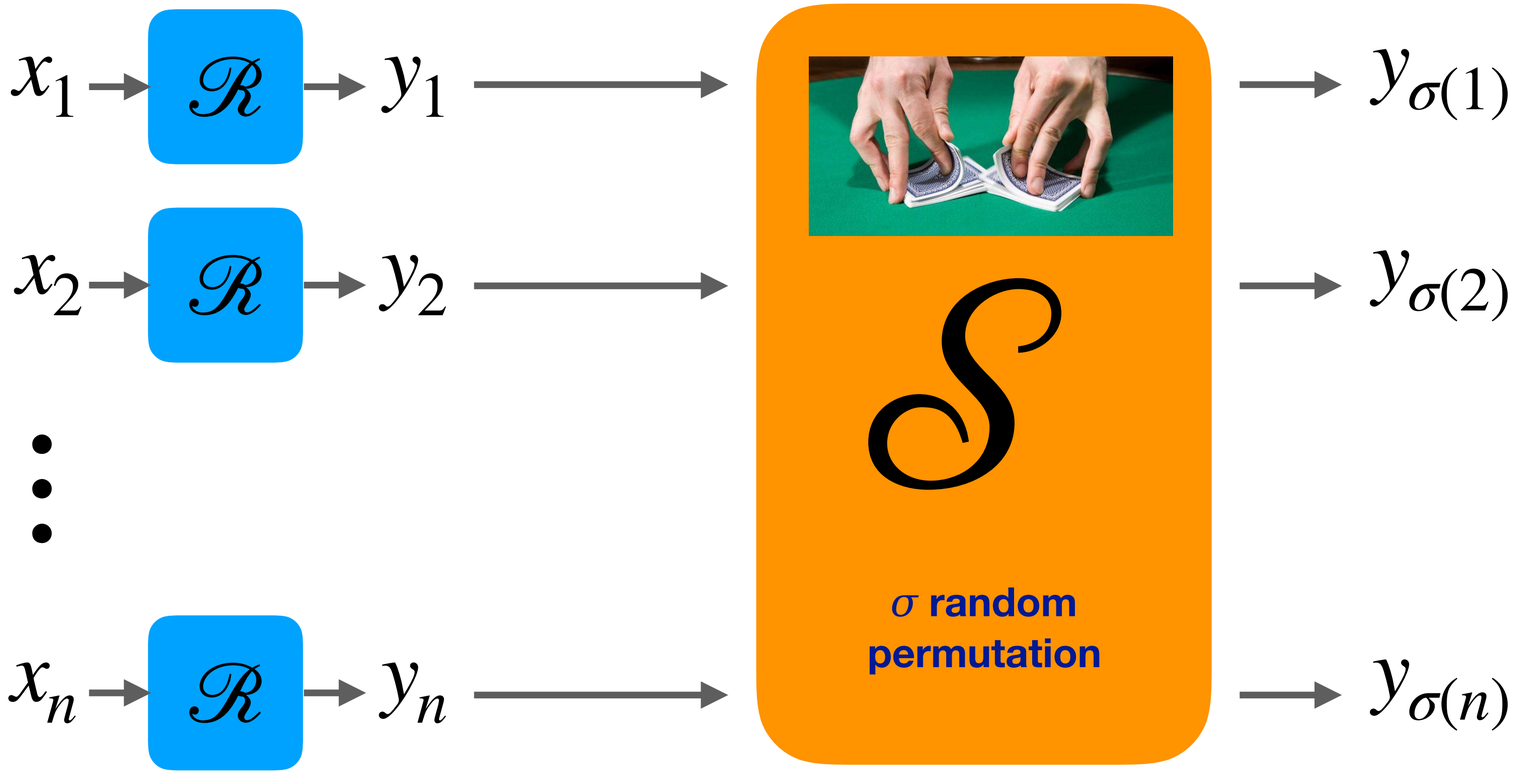
Local Randomizer

Trusted Shuffler

[BEMMRLRKTS17; EFMRTT19; CSUZZ19]

The Shuffle Model

$\mathscr{R} : \mathbb{X} \to \mathbb{Y}$ $\quad$ $\mathscr{S} : \mathbb{Y}^n \to \mathbb{Y}^n$



Privacy Analysis

$\mathscr{S} \circ \mathscr{R}^n$ $\quad$ (ε,δ)-DP

Utility Analysis

$\mathscr{A} \circ \mathscr{S} \circ \mathscr{R}^n$

[BEMMRLRKTS17; EFMRTT19; CSUZZ19]

Privacy Amplification by Shuffling

- **Problem Statement**
  - Characterize the privacy of shuffled mechanisms in terms of the privacy of its local randomizers
- **Previous Work [EFMRTT, SODA 2019]**
  - Shuffle-then-randomize (with adaptativity):

$$\varepsilon = O\left(\varepsilon_0\sqrt{\log(1/\delta)/n}\right)$$

for $\varepsilon_0 = O(1)$

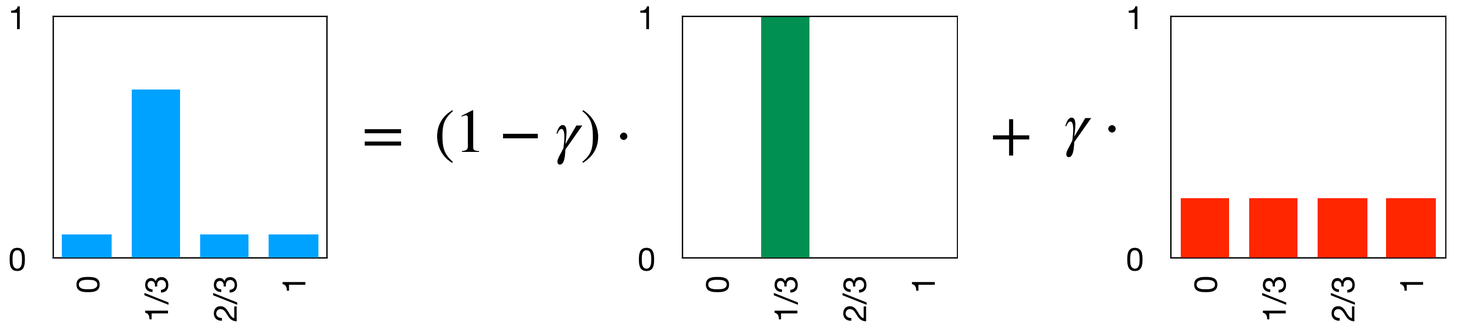
- **Our Result**
  - Randomize-then-shuffle (one randomizer):

$$\varepsilon = O\left((\varepsilon_0 \wedge 1)e^{\varepsilon_0}\sqrt{\log(1/\delta)/n}\right)$$

for $\varepsilon_0 <= 0.5 \log(n) + O(1)$

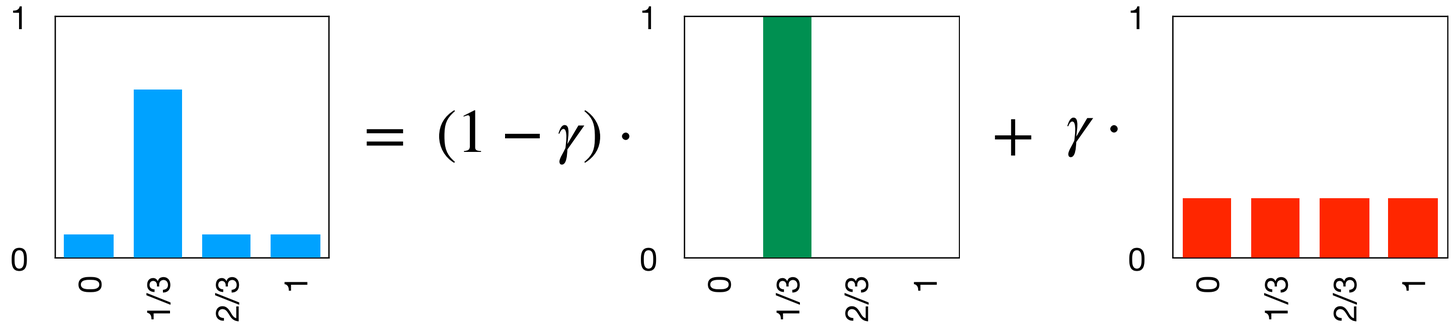
Blanket of a Local Randomizer

Randomized Response



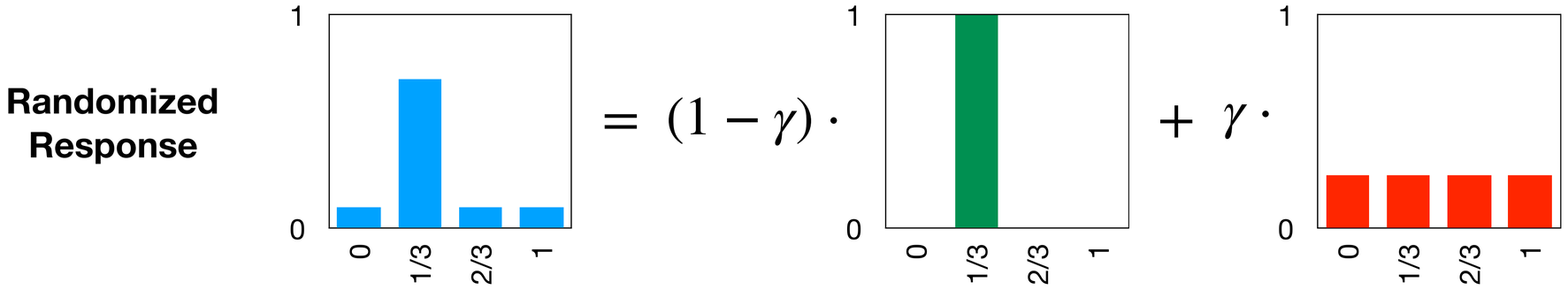
Blanket of a Local Randomizer

Randomized Response



- **Theorem (Blanket Decomposition):** Every ε_0-LDP randomizer admits a (unique maximal) mixture decomposition where one of the components is independent of the input

Blanket of a Local Randomizer



- **Theorem (Blanket Decomposition):** Every ε_0-LDP randomizer admits a (unique maximal) mixture decomposition where one of the components is independent of the input

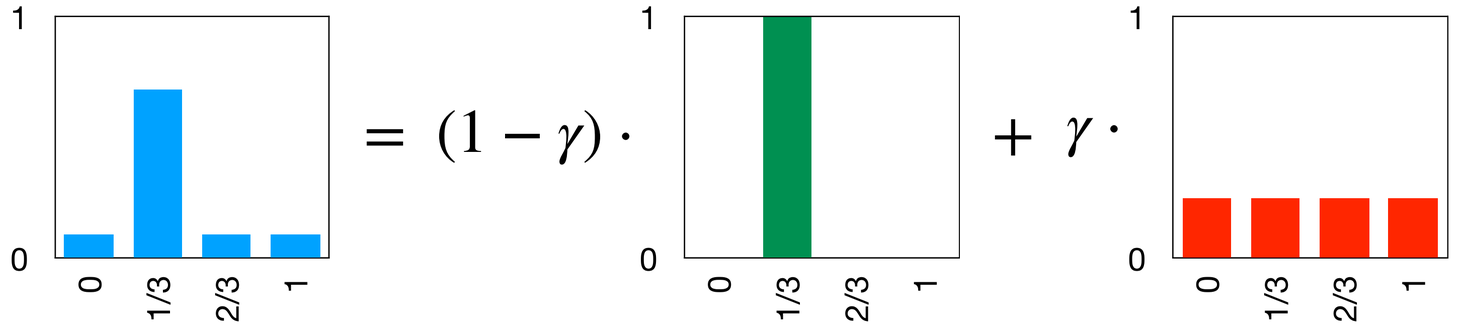
$$\mathscr{R}(x) = (1-\gamma)\mathscr{R}'(x) + \gamma\omega$$

$$\mathscr{R} : \mathbb{X} \to \mathbb{Y}$$
$$\mathscr{R}' : \mathbb{X} \to \mathbb{Y}$$
$$\omega \in Dist(\mathbb{Y})$$

$$e^{-\varepsilon_0} \leq \gamma \leq 1$$

Blanket of a Local Randomizer

Randomized Response



- **Theorem (Blanket Decomposition):** Every ε_0-LDP randomizer admits a (unique maximal) mixture decomposition where one of the components is independent of the input

$$\mathscr{R}(x) = (1-\gamma)\mathscr{R}'(x) + \gamma\omega$$

$$\mathscr{R} : \mathbb{X} \to \mathbb{Y}$$
$$\mathscr{R}' : \mathbb{X} \to \mathbb{Y}$$
$$\omega \in Dist(\mathbb{Y})$$

$$e^{-\varepsilon_0} \le \gamma \le 1$$

Blanket Construction

$$\gamma = \int_{\mathbb{Y}} \min_{x\in\mathbb{X}} p_{\mathscr{R}(x)}(y)dy$$

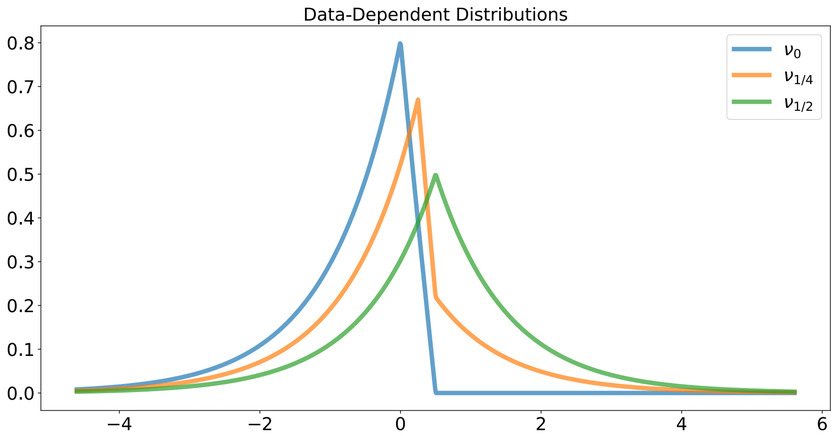
$$p_\omega(y) = \frac{\min_{x\in\mathbb{X}} p_{\mathscr{R}(x)}(y)}{\gamma}$$

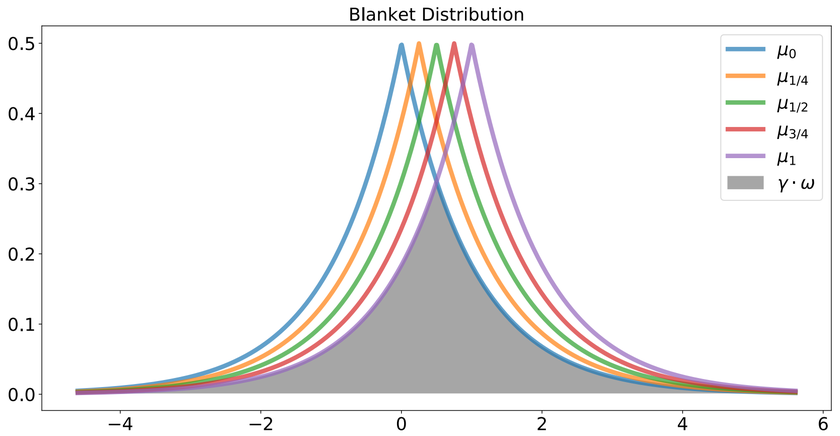
Example Blanket Decompositions

ε_0-LDP RR on [k] $\quad \gamma = \dfrac{k}{e^{\varepsilon_0} + k - 1}$

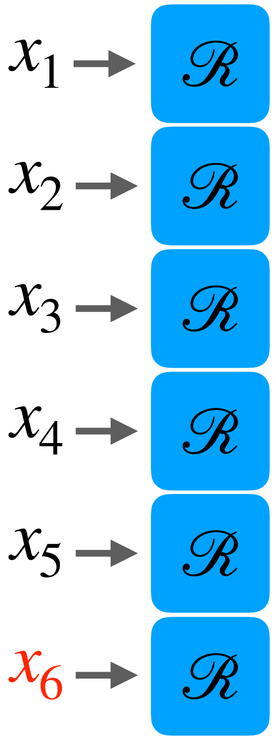
ε_0-LDP Laplace on [0,1] $\quad \gamma = e^{-\frac{\varepsilon_0}{2}}$

σ^2 Gaussian on [0,1] $\quad \gamma = 2\mathbb{P}[N(0,\sigma^2) \leq -1/2]$

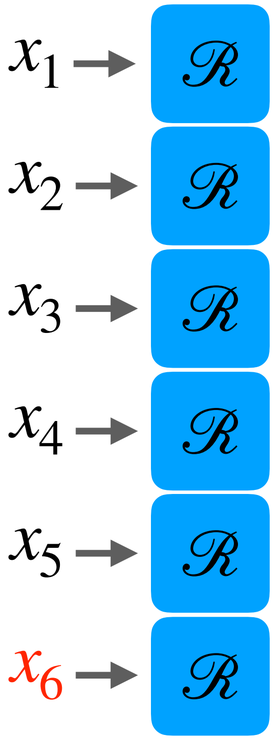


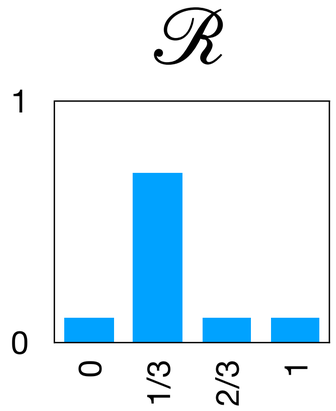


Coupling the Blankets

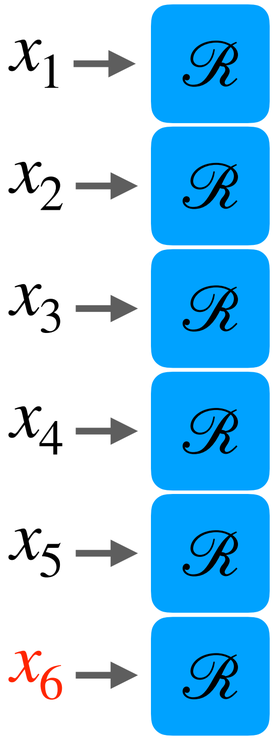


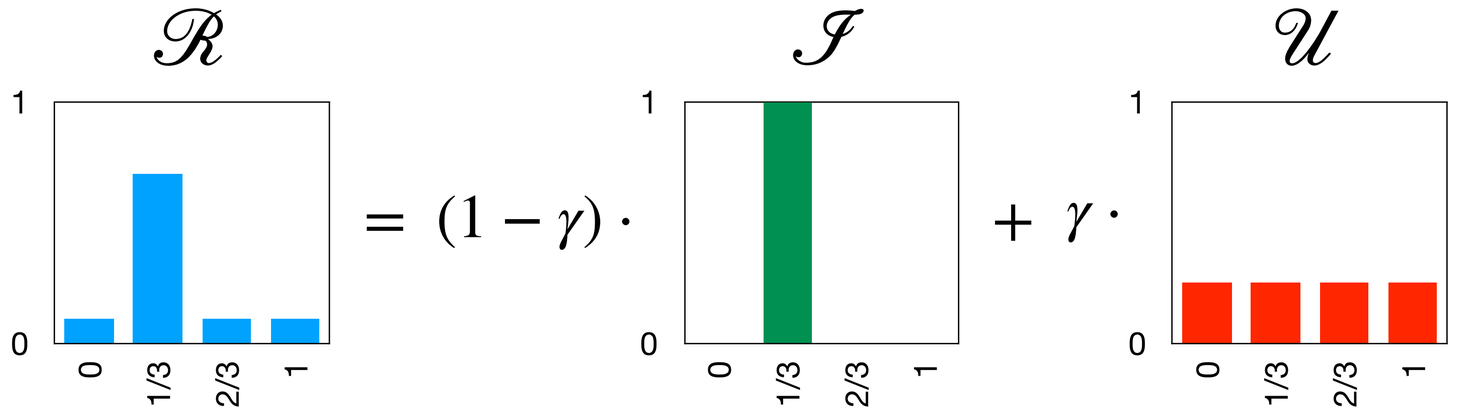
Coupling the Blankets



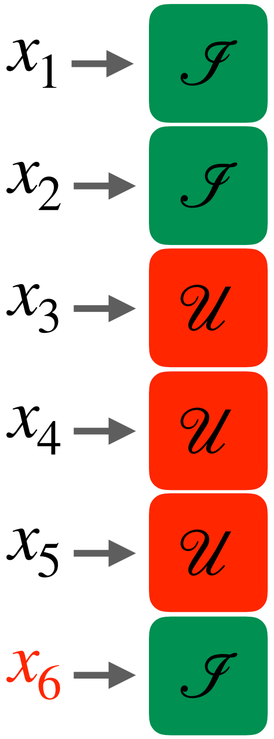


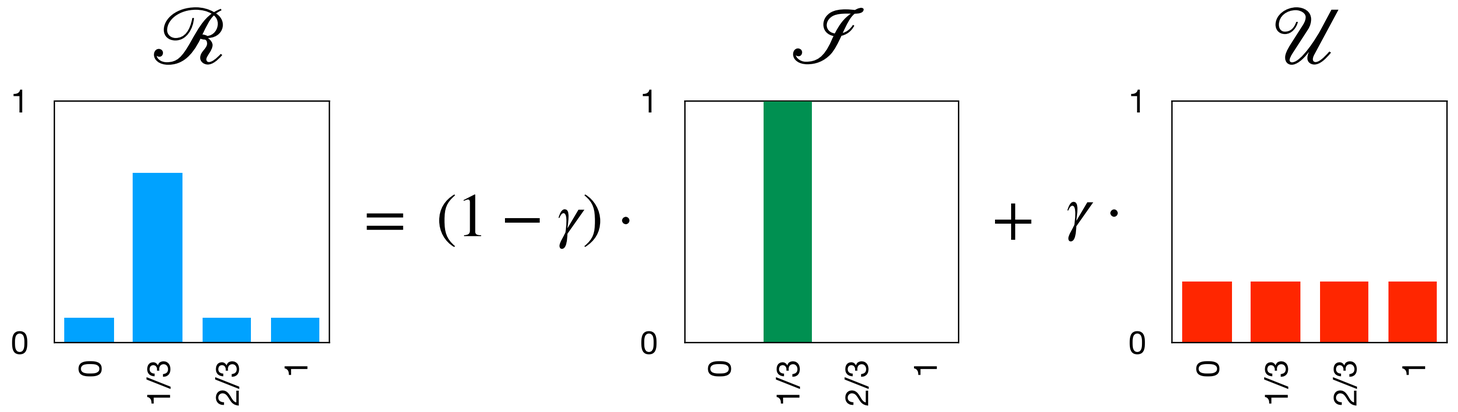
Coupling the Blankets



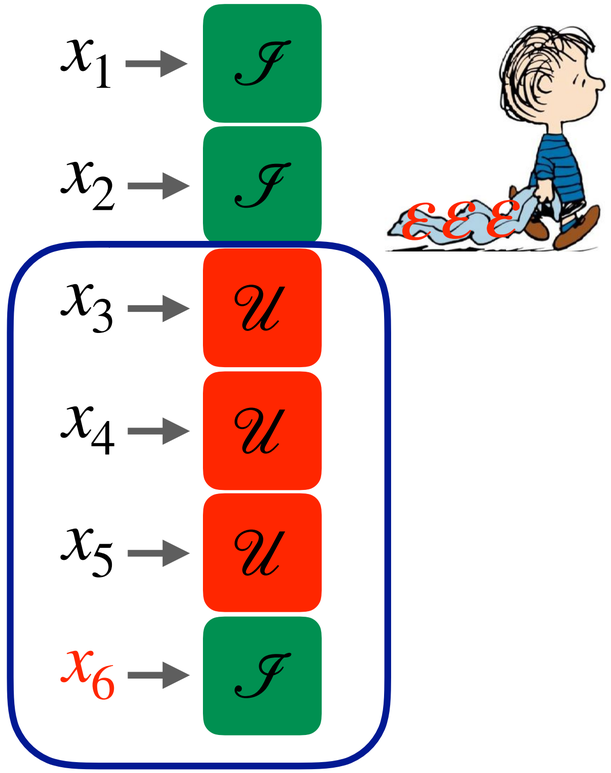


Coupling the Blankets

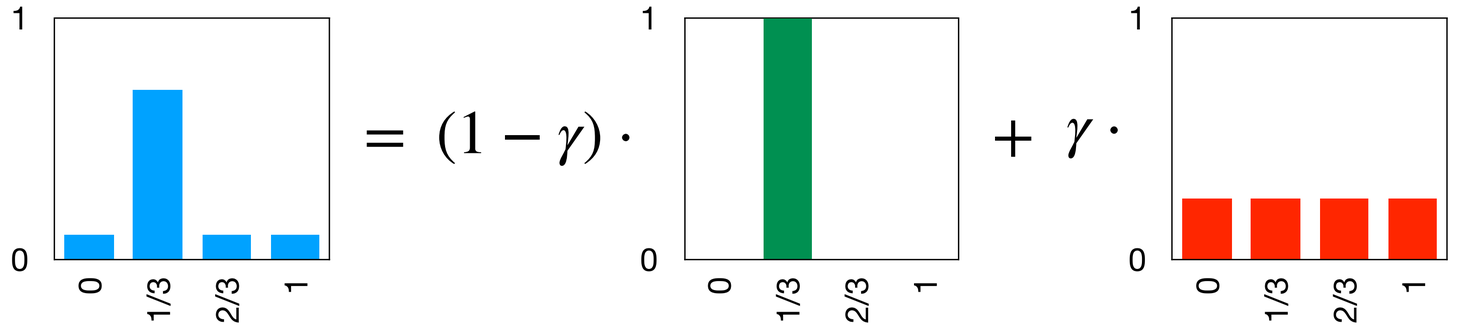




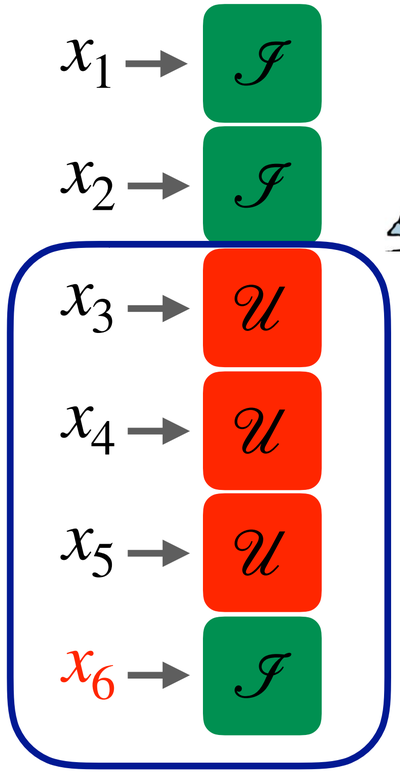
Coupling the Blankets

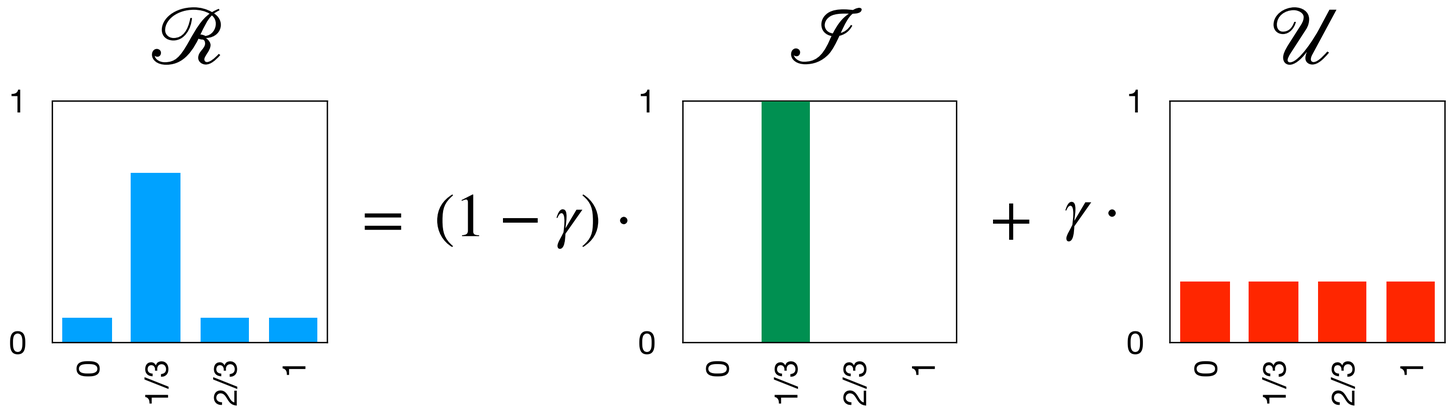


$$\mathscr{R} \quad \mathscr{I} \quad \mathscr{U}$$

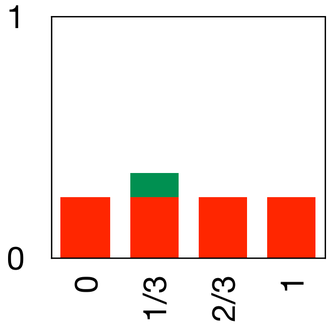


Coupling the Blankets

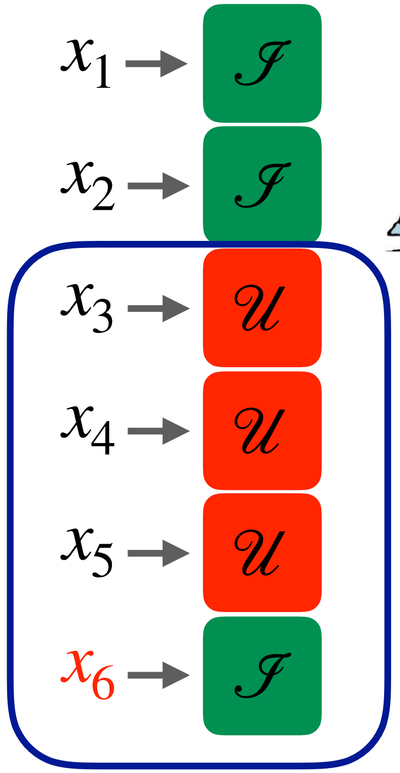


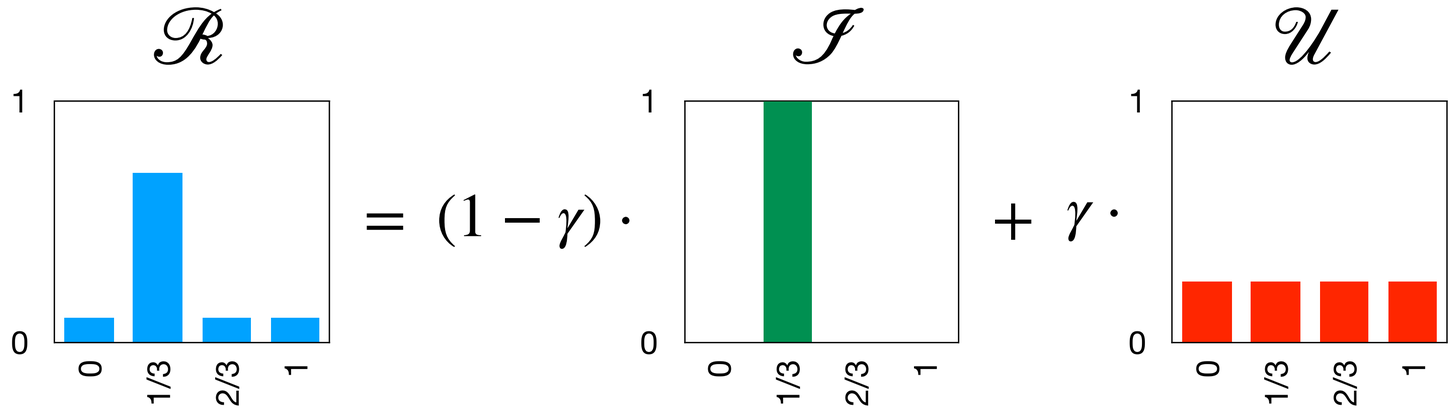


x_n and blanket

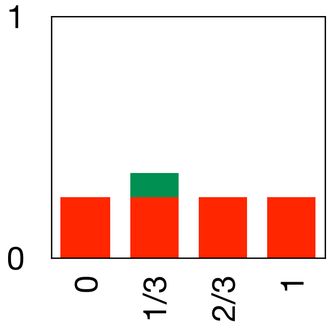


Coupling the Blankets

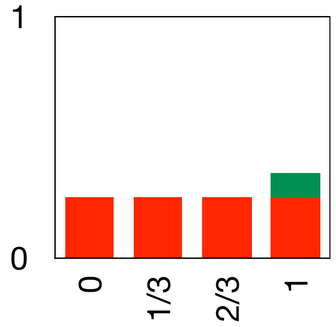




x_n and blanket



x'_n and blanket



Amplification by Shuffling

- **Theorem:** Shuffling n copies of any ε_0-LDP randomizer with blanket parameter γ gives (ε,δ)-DP with

$$\frac{\gamma(e^{\varepsilon}+1)^2(e^{\varepsilon_0}-e^{-\varepsilon_0})^2}{4n(e^{\varepsilon}-1)}\cdot\exp\left(-0.86n\left(\gamma\wedge\frac{(e^{\varepsilon}-1)^2}{\gamma(e^{\varepsilon}+1)^2(e^{\varepsilon_0}-e^{-\varepsilon_0})^2}\right)\right)\leq\delta$$

Amplification by Shuffling

- **Theorem:** Shuffling n copies of any ε_0-LDP randomizer with blanket parameter γ gives (ε,δ)-DP with

$$\frac{\gamma(e^{\varepsilon}+1)^2(e^{\varepsilon_0}-e^{-\varepsilon_0})^2}{4n(e^{\varepsilon}-1)}\cdot\exp\left(-0.86n\left(\gamma\wedge\frac{(e^{\varepsilon}-1)^2}{\gamma(e^{\varepsilon}+1)^2(e^{\varepsilon_0}-e^{-\varepsilon_0})^2}\right)\right)\leq\delta$$

- **Corollary:** Shuffling n copies of an ε_0-LDP randomizer gives (ε,δ)-DP with

$$\varepsilon=O\left((\varepsilon_0\wedge 1)e^{\varepsilon_0}\sqrt{\log(1/\delta)/n}\right)\qquad\qquad\varepsilon_0\leq\log(n/\log(1/\delta))/2$$

Amplification: Proof Idea

- General idea
  - **Couple** who samples from the blanket in both executions
  - **Reveal** the identity of who samples from the blanket (joint convexity)
  - **Remove** the data from the users in 1…n-1 who sampled from R' (post-processing)

- Define privacy amplification random variable

$$\mathbb{E}[L] = 1 - e^{\varepsilon} < 0$$

$$Y \sim \omega \qquad L = L^{\mathscr{R}}_{x,x'} = \frac{p_{\mathscr{R}(x)}(Y) - e^{\varepsilon} p_{\mathscr{R}(x')}(Y)}{p_{\omega}(Y)}$$

$$\gamma(e^{-\varepsilon_0} - e^{\varepsilon+\varepsilon_0}) \leq L \leq \gamma(e^{\varepsilon_0} - e^{\varepsilon-\varepsilon_0})$$

- Reduce to bounding expectation, apply concentration for bounded r.v.'s

$$\sup_{E} \left(\mathbb{P}[\mathcal{S} \circ \mathscr{R}^n(\overrightarrow{x}) \in E] - e^{\varepsilon} \mathbb{P}[\mathcal{S} \circ \mathscr{R}^n(\overrightarrow{x}') \in E] \right) \leq \frac{1}{\gamma n} \mathbb{E} \left[\sum_{i=1}^{Bin(n,\gamma)} L_i \right]_+$$

Getting the Bound

- Applying Hoeffding's inequality we get

$$\frac{1}{\gamma n}\mathbb{E}\left[\sum_{i=1}^{Bin(n,\gamma)} L_i\right]_+ \leq \frac{\gamma(e^{\varepsilon}+1)^2(e^{\varepsilon_0}-e^{-\varepsilon_0})^2}{4n(e^{\varepsilon}-1)} \cdot \exp\left(-0.86n\left(\gamma \wedge \frac{(e^{\varepsilon}-1)^2}{\gamma(e^{\varepsilon}+1)^2(e^{\varepsilon_0}-e^{-\varepsilon_0})^2}\right)\right)$$

- Refinements:
  - Use mechanism-specific bounds on L and γ
  - Alternative concentration bounds, eg. Bennett's inequality

Amplification by Iteration in NoisySGD

Algorithm 1: Noisy Projected Stochastic Gradient Descent — NoisyProjSGD$(D, \ell, \eta, \sigma, \xi_0)$

Input: Dataset $D = (z_1, \ldots, z_n)$, loss function $\ell : \mathbb{K} \times \mathbb{D} \to \mathbb{R}$, learning rate η, noise parameter σ, initial distribution $\xi_0 \in \mathcal{P}(\mathbb{K})$

Sample $x_0 \sim \xi_0$

for $i \in [n]$ **do**

  $x_i \leftarrow \Pi_{\mathbb{K}}\left(x_{i-1} - \eta(\nabla_x \ell(x_{i-1}, z_i) + Z)\right)$ with $Z \sim \mathcal{N}(0, \sigma^2 I)$

return x_n

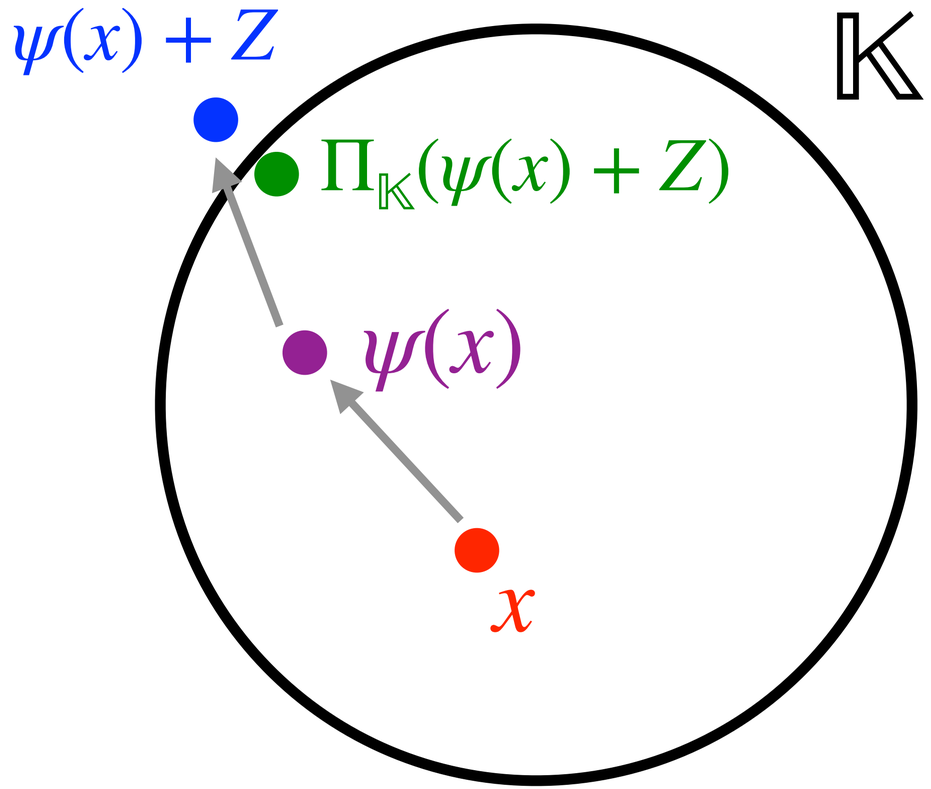
- If D and D' differ in position j, then the last n-j iterations are postprocessing
  - Can also use public data for the last r iterations
- Start from a coupling between x_j and x_j' and propagate it through
  - Keep all the mass as close to the diagonal as possible

[FMTT'18]

Projected Generalized Gaussian Mechanism

$$K(x) = \Pi_{\mathbb{K}}(\mathcal{N}(\psi(x), \sigma^2 I))$$

$$\psi : \mathbb{R}^d \to \mathbb{R}^d$$



Amplification by Coupling

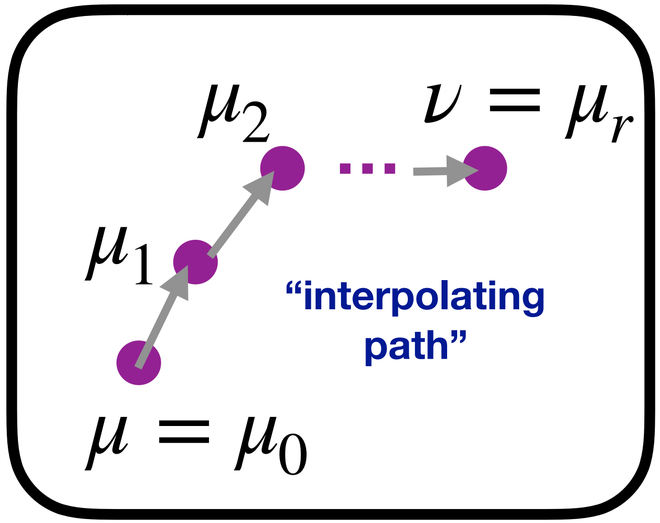
Suppose $\psi_1, \ldots, \psi_r$ are L-Lipschitz

$$K_i(x) = \Pi_{\mathbb{K}}(\mathcal{N}(\psi_i(x), \sigma^2 I))$$

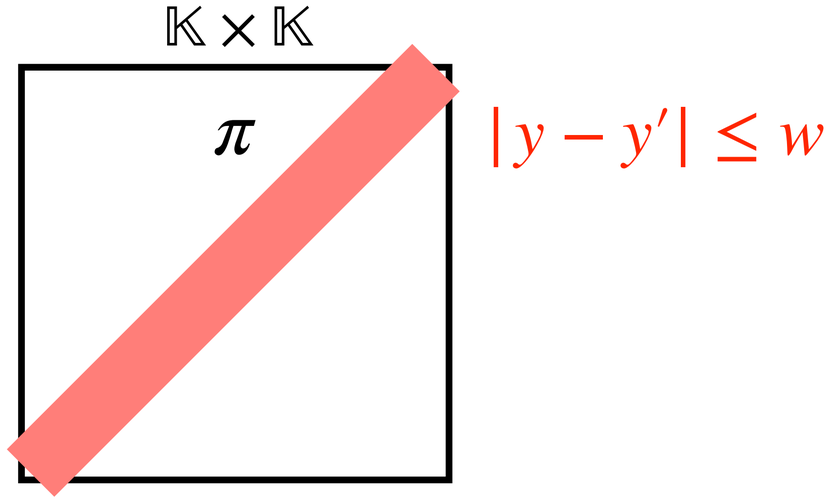
$$\mathrm{R}_\alpha(\mu K_1 \cdots K_r \| \nu K_1 \cdots K_r) \leq \frac{\alpha L^2}{2\sigma^2} \sum_{i=1}^{r} L^{2(r-i)} \mathrm{W}_\infty(\mu_i, \mu_{i-1})^2$$

Rényi Divergence **Wasserstein Distance**

$\mathscr{P}(\mathbb{K})$



Applications:
- Bound L
- Optimize path



[BBGG'19]

Per-index RDP in NoisySGD

Suppose the loss is Lipschitz and smooth

*If loss is **convex** can take L=1. Then i-th person receives $\varepsilon_i(\alpha)$-RDP with*

$$\epsilon_i(\alpha) = O\left(\frac{\alpha}{(n-i)\sigma^2}\right)$$

[FMTT'18]

*If loss is **strongly convex** can take L< 1. Then i-th person receives $\varepsilon_i(\alpha)$-RDP with*

$$\epsilon_i(\alpha) = O\left(\frac{\alpha L^{(n-i)/2}}{(n-i)\sigma^2}\right)$$

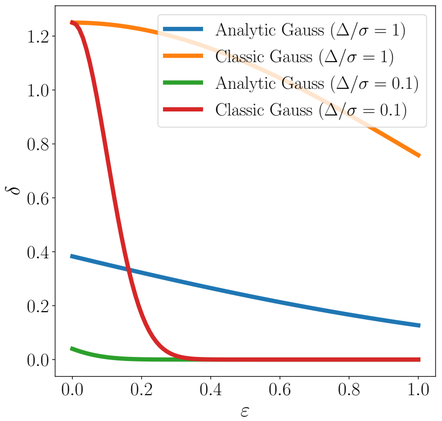
[BBGG'19]

Summary

- Couplings (including overlapping mixtures) provide a powerful methodology to study privacy amplification in many settings
  - Including: subsampling, postprocessing, shuffling and iteration
- Properties of divergences related to (R)DP (eg. advanced joint convexity) are “necessary” to get tight amplification bounds
- Different types of couplings are useful (eg. maximal and small distance)

Conclusion

- **In DP constants (and exact expressions) matter**
  - Better noise calibration => better utility
  - See also the “analytic Gaussian mechanism” *[BW’18]*



- **Make every bit of randomness count!**
  - Does your postprocessing improve privacy?
- **Other types of privacy amplification?**
  - Eg. is Report Noisy Max an instance of privacy amplification?