The Composition Theorem for Differential Privacy

Peter Kairouz, Sewoong Oh, and Pramod Viswanath
E-mails: {kairouz2,swoh,pramodv}@illinois.edu
University of Illinois at Urbana Champaign, USA

Statistical Data Privacy

Privacy via plausible deniability:

have you ever used illegal drugs?

say yes | answer truthfully

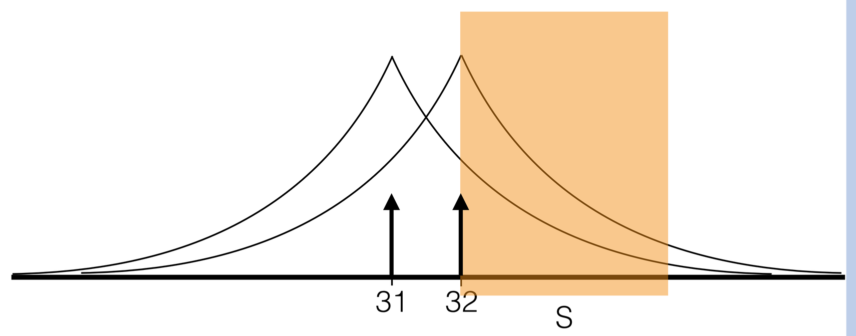
(ε, δ)-differential privacy:

D_0

Alice	22
Bob	45
⋮	⋮
Me	23

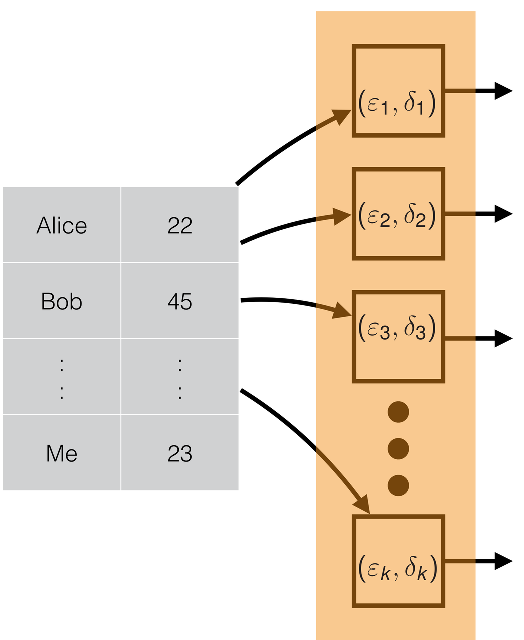
D_1

Alice	22
Bob	45
⋮	⋮



$$\mathbb{P}(q(D_0) \in S) \le e^{\varepsilon}\, \mathbb{P}(q(D_1) \in S) + \delta$$

Composition attacks:



how much privacy is lost in the end?

$$\left(\sum_{i=1}^{k} \varepsilon_i, \sum_{i=1}^{k} \delta_i\right)$$

what if we allow for some slack $\tilde{\delta} > 0$?

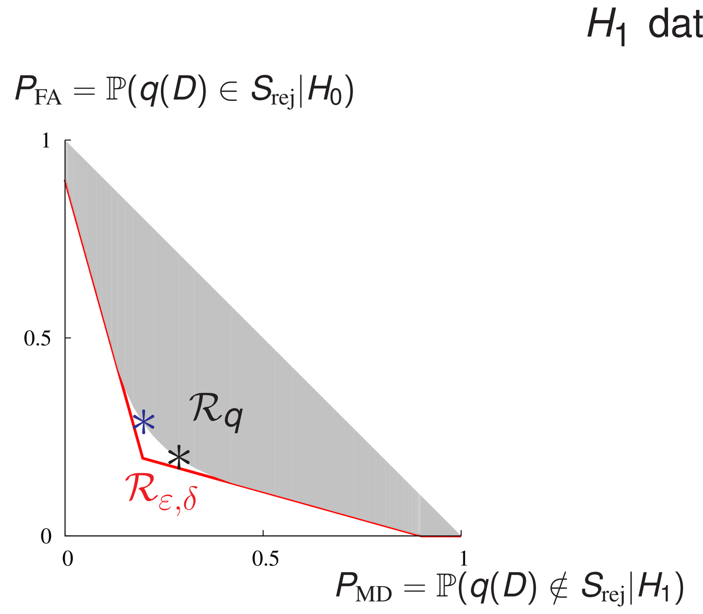
If $\left(\varepsilon_i = \varepsilon, \delta_i = \delta\right)$, then $\left(k\varepsilon^2 + \varepsilon\sqrt{k \log(1/\tilde{\delta})}, k\delta + \tilde{\delta}\right)$

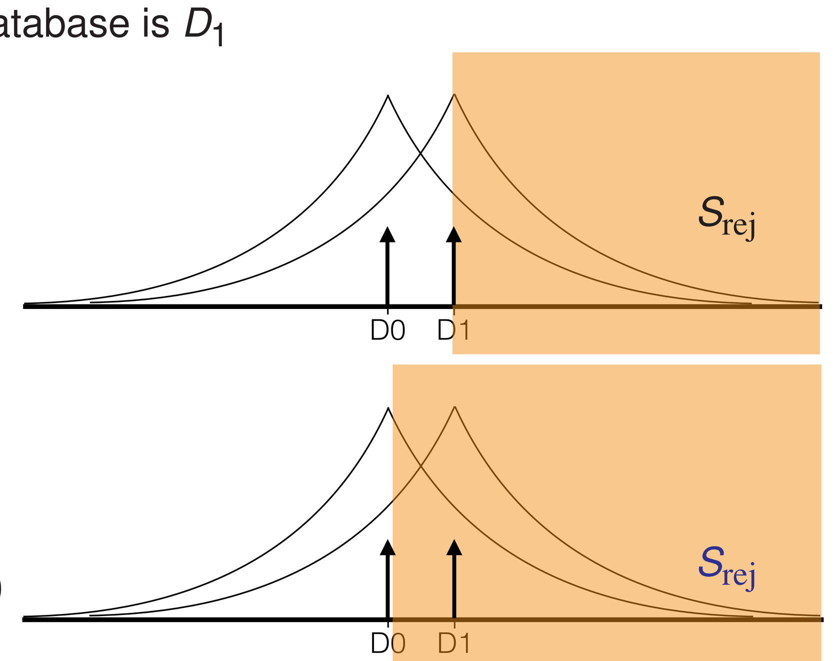
Connections to Hypothesis Testing

Privacy region of a privatization mechanism:

- fix a privatization mechanism q

H_0 database is D_0
H_1 database is D_1





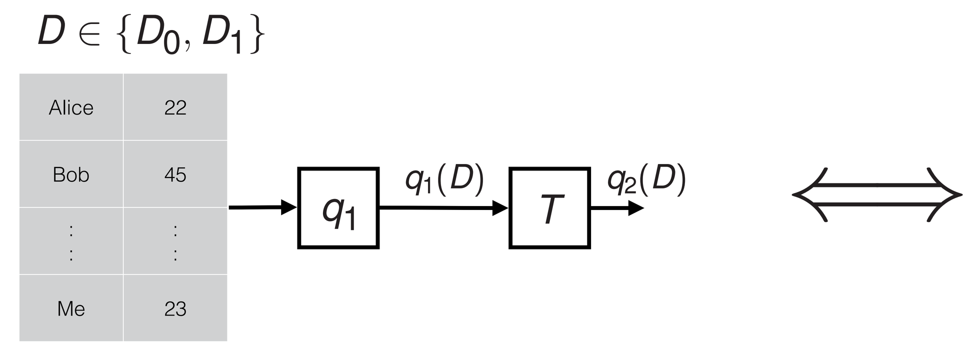
Operational Definition of Differential Privacy [Kairouz, Oh, Viswanath '15]

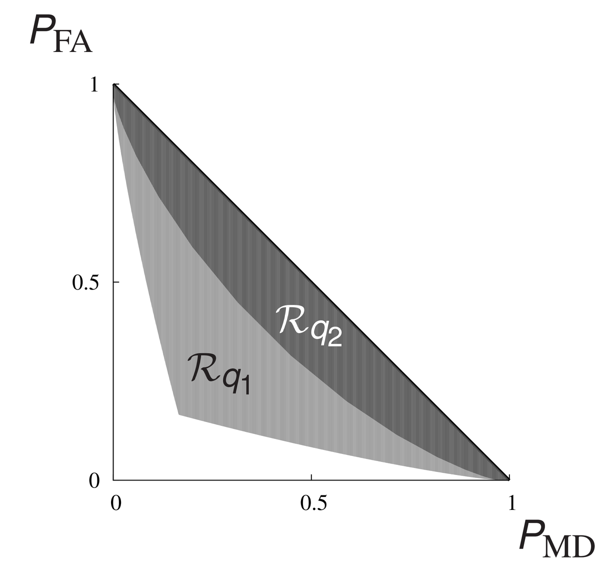
q is (ε, δ)-differentially private $\iff$ $\mathcal{R}_q \subseteq \mathcal{R}_{\varepsilon,\delta}$

$$P_{\rm FA} + e^{\varepsilon} P_{\rm MD} \ge 1 - \delta$$
$$e^{\varepsilon} P_{\rm FA} + P_{\rm MD} \ge 1 - \delta$$

The Optimality of the Randomized Response Mechanism

Data processing inequality & its converse:



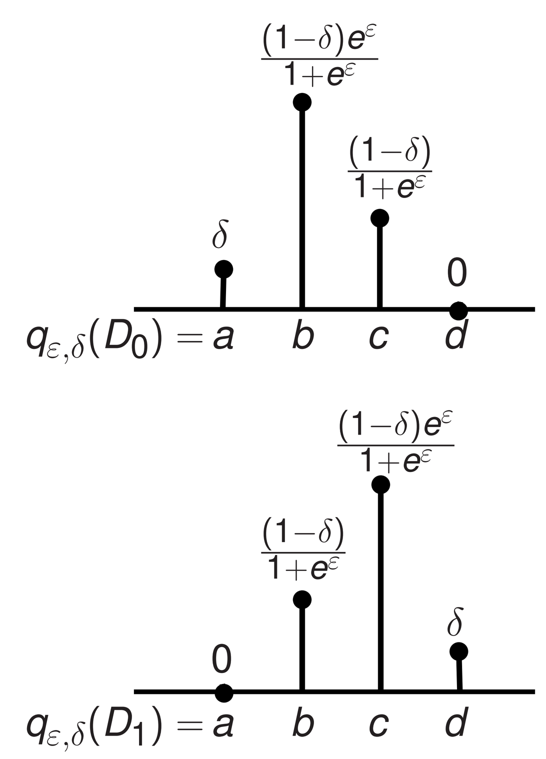


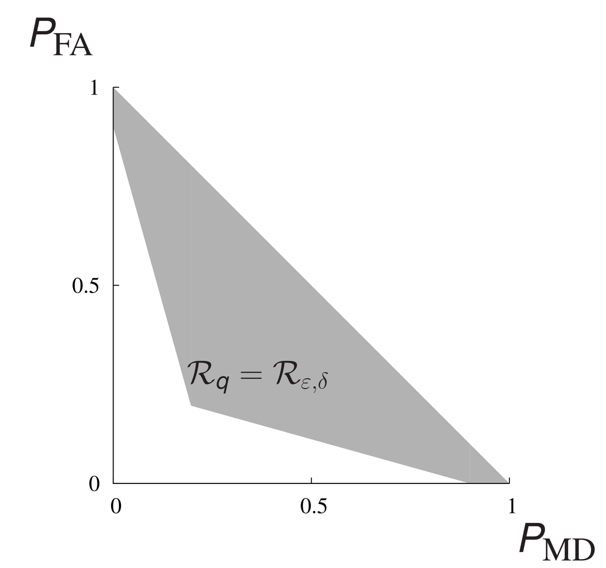
The Data Processing Inequality and its Converse [Kairouz, Oh, Viswanath '15]

$$D–q_1(D)–q_2(D) \iff \mathcal{R}_{q_2} \subseteq \mathcal{R}_{q_1}$$

- precisely, if $\mathcal{R}_{q_2} \subseteq \mathcal{R}_{q_1}$ then there exists a coupling of $q_1(D)$ and $q_2(D)$ such that
  - (a) $D–q_1(D)–q_2(D)$ or equivalently
  - (b) $q_2(D) = T(\,q_1(D)\,)$

The randomized response mechanism:



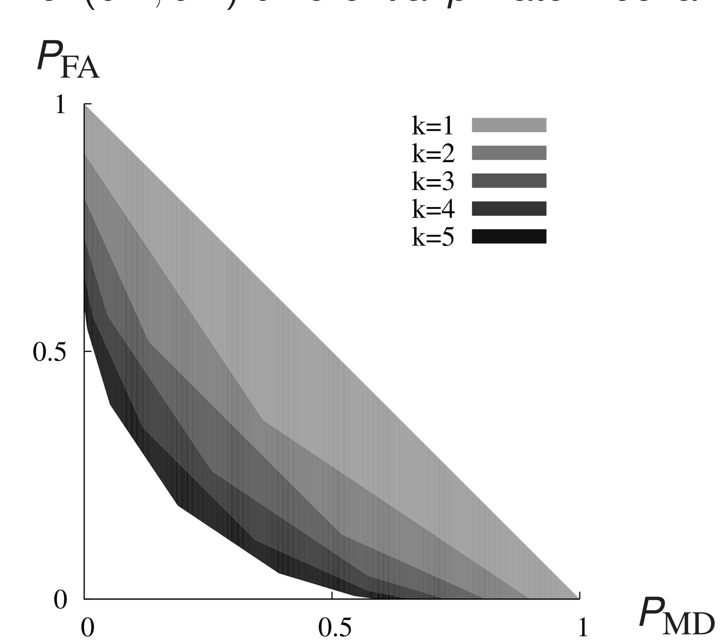


The Optimality of the Randomized Response Mechanism

The randomized response $q_{\varepsilon,\delta}$ dominates over all (ε, δ)-differentially private mechanisms.

Composition under the randomized response mechanism:

k composition of $(0.4, 0.1)$-differential private mechanisms



- this gives the exact evolution of privacy

The Composition Theorem

Optimal privacy under composition of homogenous mechanisms:

The Composition Theorem I [Kairouz, Oh, Viswanath '15]

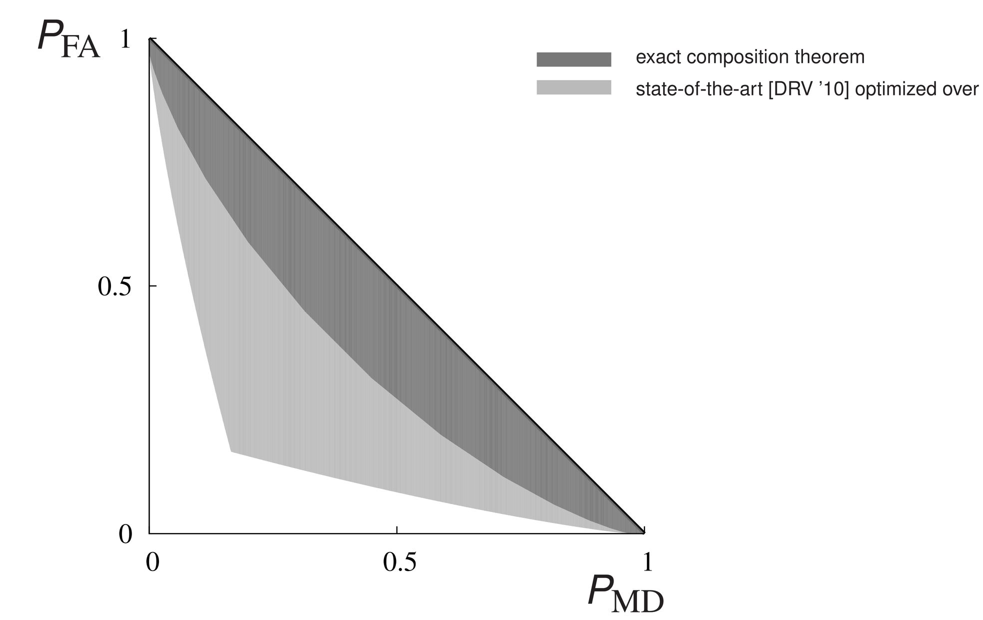
The k-fold composition of (ε, δ)-differentially private mechanisms satisfies $(\tilde{\varepsilon}_{\tilde{\delta}}, k\delta + \tilde{\delta})$-differential privacy with

$$\tilde{\varepsilon}_{\tilde{\delta}} = \min\left\{ k\varepsilon \;,\; k\varepsilon^2 + \sqrt{k\varepsilon^2 \log(e + 1/\tilde{\delta})} \right\}$$

- significant improvement over $(k\varepsilon, k\delta)$-guarantee when $\varepsilon \to 0$

Comparisons with the state-of-the-art results:

30-fold composition of $(0.1, 0.001)$-differentially private mechanisms



Optimal privacy under composition of heterogeneous mechanisms:

The Composition Theorem II [Kairouz, Oh, Viswanath '15]

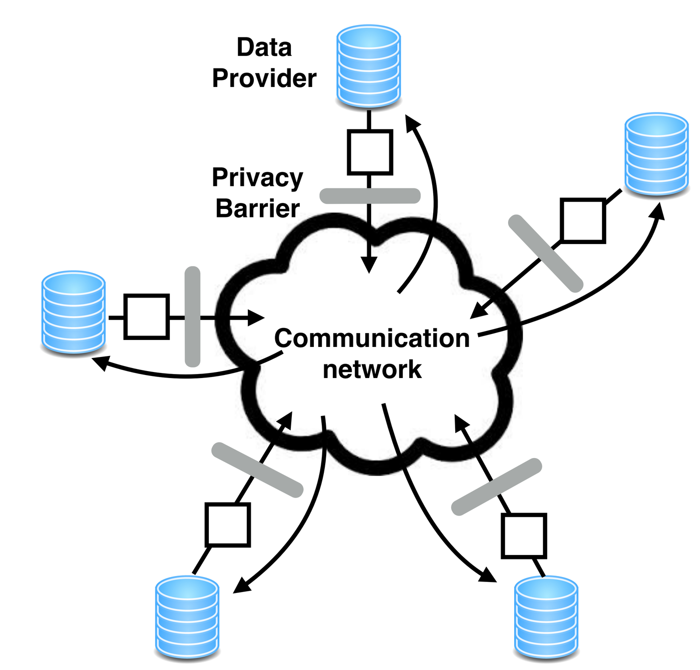
For any $\varepsilon_\ell > 0$, $\delta_\ell \in [0,1]$ for $\ell \in \{1, \dots, k\}$, and $\tilde{\delta} \in [0,1]$, the class of $(\varepsilon_\ell, \delta_\ell)$-differentially private mechanisms satisfy $(\tilde{\varepsilon}_{\tilde{\delta}}, 1 - (1-\tilde{\delta})\prod_{\ell=1}^{k}(1-\delta_\ell))$-differential privacy under k-fold adaptive composition, for $\tilde{\varepsilon}_{\tilde{\delta}} =$

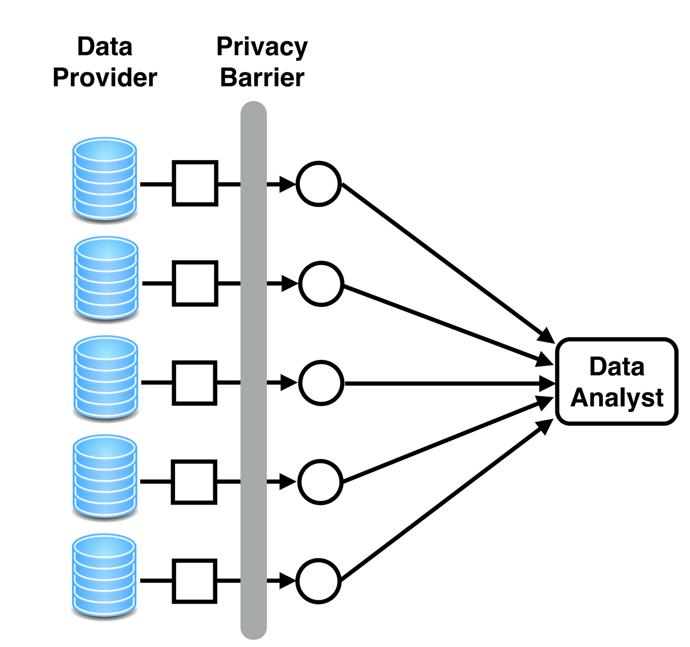
$$\min\left\{ \sum_{\ell=1}^{k} \varepsilon_\ell \;,\; k\tilde{\varepsilon}^2 + \sqrt{2\,k\,\tilde{\varepsilon}^2 \log\left(e + \sqrt{k}\tilde{\varepsilon}/\tilde{\delta}\right)} \right\},$$

where $\tilde{\varepsilon}^2 = \frac{1}{k}\sum_{\ell=1}^{k} \varepsilon_\ell^2$ for $\varepsilon \le 1/2$.

Going Forward

- Computational Complexity [Vadhan, Murtagh '15]





- *"Optimality of non-interactive randomized response"*, arXiv:1407.1546
- *"Extremal Mechanisms for Local Differential Privacy"*, arXiv:1407.1338

International Conference on Machine Learning (ICML), July 2015