The Composition Theorem for Differential Privacy

Peter Kairouz, Sewoong Oh, and Pramod Viswanath
E-mails: [kairouz,gowh,pramody]@illinois.edu
University of Illinois at Urbana Champaign, USA

International Conference on Machine Learning (ICML), July 2015

The Composition Theorem

Optimal privacy under composition of homogenous mechanisms:

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

The k-fold composition of $(\epsilon, \delta)$-differentially private mechanisms satisfies $(\epsilon, k\delta + \delta)$-differential privacy with

$$
\epsilon' = \min \left\{ \epsilon : k \epsilon^2 + \sqrt{k^2 \log(1/\delta)} \right\}
$$

Significant improvement over $(\epsilon, k\delta)$-guarantees when $k \to 0$

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

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

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

For any $\epsilon, 0, \delta \in [0, 1]$ for $k \in \{1, \ldots, k\}$, and $\delta \in [0, 1]$, the class of $(\epsilon, \delta)$-differentially private mechanisms satisfy $(\epsilon, 1 - (1 - \delta)^k \prod_{i=1}^k (1/\delta_i))$-differential privacy under k-fold adaptive composition, for $\epsilon' = \min \left\{ \epsilon : k \epsilon^2 + \sqrt{k^2 \log(1/\delta)} \right\}$,

$$
\epsilon' = \frac{\epsilon}{\left(1 - \delta\prod_{i=1}^k (1/\delta_i)\right)^{1/k}}
$$

where $\epsilon' = \frac{\epsilon}{\left(1 - \delta\prod_{i=1}^k (1/\delta_i)\right)^{1/k}}$ for $\epsilon \leq 1/2$.

Going Forward

- Computational Complexity [Vadhan, Murtagh ’15]