Privacy via plausible deniability: have you ever used illegal drugs?

Composition attacks:

<table>
<thead>
<tr>
<th>Data Provider</th>
<th>Privacy Barrier</th>
<th>Communication network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Me</td>
<td>23</td>
<td></td>
</tr>
</tbody>
</table>

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

The randomized response mechanism:

The Optimality of the Randomized Response Mechanism

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

q is $(\epsilon, \delta)$-differentially private

The Composition Theorem

Optimal privacy under composition of heterogeneous mechanisms:

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

For any $\epsilon_j > 0, \delta_j \in [0, 1]$ for $j \in \{1, \ldots, k\}$, and $\delta \in [0, 1]$, the class of $(\epsilon_j, \delta_j)$-differentially private mechanisms satisfy $\epsilon = \min_{j=1}^{k} (\epsilon_j, 1 - (1 - \delta_j))$-differential privacy under k-fold adaptive composition, for $\epsilon = 0$:

$$
\epsilon = \min_{j=1}^{k} (\epsilon_j, 1 - (1 - \delta_j)) = \min_{j=1}^{k} (\epsilon_j, \delta_j)
$$


The Optimality of the Randomized Response Mechanism

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

Composition under the randomized response mechanism:

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

Statistical Data Privacy

Privacy via plausible deniability:

Composition of heterogeneous mechanisms:

Composition under the randomized response mechanism:

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

Optimal privacy under composition of homogenous mechanisms:

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

Computational Complexity [Vadhan, Murtagh '15]

Optimal privacy under composition of heterogeneous mechanisms:

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 $(\epsilon^\prime, k \delta + \delta')$-differential privacy with

$$
\epsilon^\prime = \min \left\{ \epsilon, k \epsilon^2 + \sqrt{k \epsilon^2 \log(e + 1)}, k \epsilon + \delta \right\}
$$

Computations under the randomized response mechanism:

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

Composition under the randomized response mechanism:

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

this gives the exact evolution of privacy