The Complexity of Privacy and Polynomial Approximations
or: How I Learned to Stop Worrying and Love Lower Bounds

Mark Bun, Harvard
January 11, 2016
ITCS ‘16 Graduating Bits
Lower Bounds in Differential Privacy

$d$ binary attributes

<table>
<thead>
<tr>
<th>DarkSide?</th>
<th>Twin?</th>
<th>Skywalker?</th>
<th>&lt; 3ft?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

$n$ people

\[
\begin{align*}
\text{1/4} & + & \text{1/2} & + & \text{3/4} & + & \text{1/4} & + \\
\text{Noise} & + & \text{Noise} & + & \text{Noise} & + & \text{Noise} & \\
\end{align*}
\]
Lower Bounds in Differential Privacy

\[ d \text{ binary attributes} \]

<table>
<thead>
<tr>
<th></th>
<th>DarkSide?</th>
<th>Twin?</th>
<th>Skywalker?</th>
<th>&lt; 3ft?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 0, 0</td>
<td>0, 0, 0</td>
<td>0, 1, 1</td>
<td>0, 1, 0</td>
<td>1, 0, 0</td>
</tr>
<tr>
<td>0, 0, 0</td>
<td>0, 1, 0</td>
<td>1, 1, 0</td>
<td>0, 0, 0</td>
<td>0, 0, 0</td>
</tr>
<tr>
<td>0, 0, 0</td>
<td>0, 1, 0</td>
<td>1, 1, 0</td>
<td>0, 0, 0</td>
<td>0, 0, 0</td>
</tr>
<tr>
<td>1, 0, 0</td>
<td>0, 1, 1</td>
<td>0, 1, 0</td>
<td>1, 0, 0</td>
<td>0, 0, 0</td>
</tr>
</tbody>
</table>

\[ \frac{1}{4} + \text{Noise} \]
\[ \frac{1}{2} + \text{Noise} \]
\[ \frac{3}{4} + \text{Noise} \]
\[ \frac{1}{4} + \text{Noise} \]

Less error

Insufficient for DP

\[ \text{Noise} \leq \min\{d, n\}^{1/2}/n \]

[KRSU10]

More error

Suffices for DP

\[ \text{Noise} \geq \frac{d^{1/2}}{n} \]

[DN03, DN04, BDMN05, DMNS06]
**Lower Bounds in Differential Privacy**

A table showing the binary attributes for different personas:

<table>
<thead>
<tr>
<th></th>
<th>DarkSide?</th>
<th>Twin?</th>
<th>Skywalker?</th>
<th>&lt; 3ft?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

For $d$ binary attributes and $n$ people, the noise required for differential privacy (DP) is:

- Less error: Noise $\leq d^{1/2}/n$ [B.-Ullman-Vadhan STOC’14]
- Insufficient for DP

- More error: Noise $\geq d^{1/2}/n$ [DN03, DN04, BDMN05, DMNS06]
- Suffices for DP

Lower bound via cryptographic “fingerprinting codes” [BS95]
More lower bounds for differential privacy

**Information theoretic**

B.-Nissim-Stemmer-Vadhan FOCS’15

B.-Nissim-Stemmer Tomorrow!

**Computational**

B.-Zhandry TCC’16-A
More lower bounds for differential privacy

Information theoretic
B.-Nissim-Stemmer-Vadhan FOCS’15
B.-Nissim-Stemmer Tomorrow!

Computational
B.-Zhandry TCC’16-A

Lower bounds for approximate degree
• Tight lower bound for AND-OR tree [B.-Thaler ICALP’13]
• Techniques extend to yield lower bounds in communication cx. and learning theory

[ICALP’15]
More lower bounds for differential privacy

**Information theoretic**
B.-Nissim-Stemmer-Vadhan FOCS’15
B.-Nissim-Stemmer Tomorrow!

**Computational**
B.-Zhandry TCC’16-A

Lower bounds for *approximate degree*
• Tight lower bound for AND-OR tree [B.-Thaler ICALP’13]
• Techniques extend to yield lower bounds in communication cx. and learning theory

[Thaler ICALP’15]

Thank you!