

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


n people

	DarkSide?	Twin?	Skywalker?	< 3ft?
	0	0	0	1
	0	1	1	0
	0	1	1	0
	1	0	1	0
	1/4 + Noise	1/2 + Noise	3/4 + Noise	1/4 + Noise

Lower Bounds in Differential Privacy

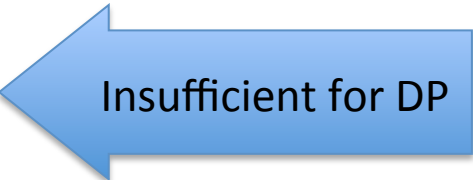
d binary attributes

n people

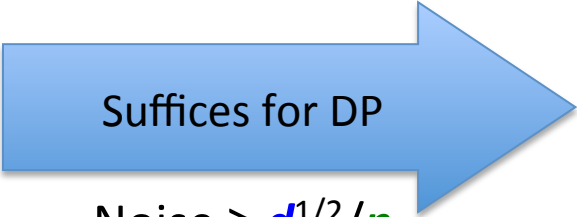
	DarkSide?	Twin?	Skywalker?	< 3ft?
	0	0	0	1
	0	1	1	0
	0	1	1	0
	1	0	1	0

1/4	1/2	3/4	1/4
+	+	+	+
Noise	Noise	Noise	Noise

Less error



Noise $\leq \min\{d, n\}^{1/2}/n$
[KRSU10]



More error

Noise $\geq d^{1/2}/n$
[DN03, DN04, BDMN05, DMNS06]

Lower Bounds in Differential Privacy

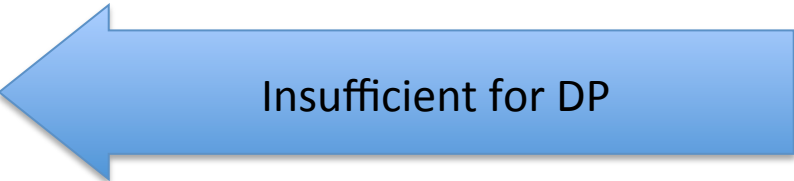
d binary attributes

n people

	DarkSide?	Twin?	Skywalker?	< 3ft?
	0	0	0	1
	0	1	1	0
	0	1	1	0
	1	0	1	0

$1/4$ $1/2$ $3/4$ $1/4$
 + + + +
 Noise Noise Noise Noise

Less error



Noise $\leq d^{1/2}/n$

[B.-Ullman-Vadhan STOC'14]



Noise $\geq d^{1/2}/n$

[DN03, DN04, BDMN05, DMNS06]

More error

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!

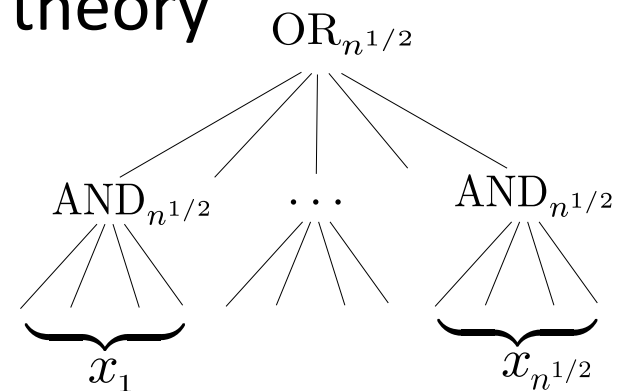
Computational

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

[B.-Thaler 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

[B.-Thaler ICALP'15]

Thank you!

