

Bridging The Gap between Theory and Practice in Data Privacy



Challenge:

- Most differentially private algorithms with utility proofs work poorly empirically
- Some algorithms work well only for settings chosen by the authors

Solution:

- Tools for semi-formal analysis of utility (similar to bias/variance tradeoff)
- Decompose algorithms in to steps, and empirically analyze effect of steps

Theory is when you know something, but it doesn't work.
Practice is when something works, but you don't know why.

- From slides by Giuseppe Italiano

“In theory, there is no difference between theory and practice. But, in practice, there is.”

- Jan L. A. van de Snepscheut

We want to find something that works, know why, and also know why something doesn't work.

Scientific Impact:

- Improve the understanding of power and limitations of DP
- Research methodology that better balances theory and practice.

Broader Impact:

- Improve deployed privacy-preservation techniques.

Number: 1640374

PI: Ninghui Li; Purdue University