Croft W, Sack JR, Shi W. Differential privacy via a truncated and normalized Laplace mechanism. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 37(2): 369-388 Mar. 2022. DOI 10.1007/s11390-020-0193-z

Differential Privacy via a Truncated and Normalized Laplace Mechanism

William Croft, Jörg-Rüdiger Sack, Wei Shi

Research Objectives

- **Problem Domain:**
  - Querying sensitive databases requires careful manipulation of query responses to protect privacy
  - Differentially private mechanisms add controlled noise to query responses to provide a privacy guarantee

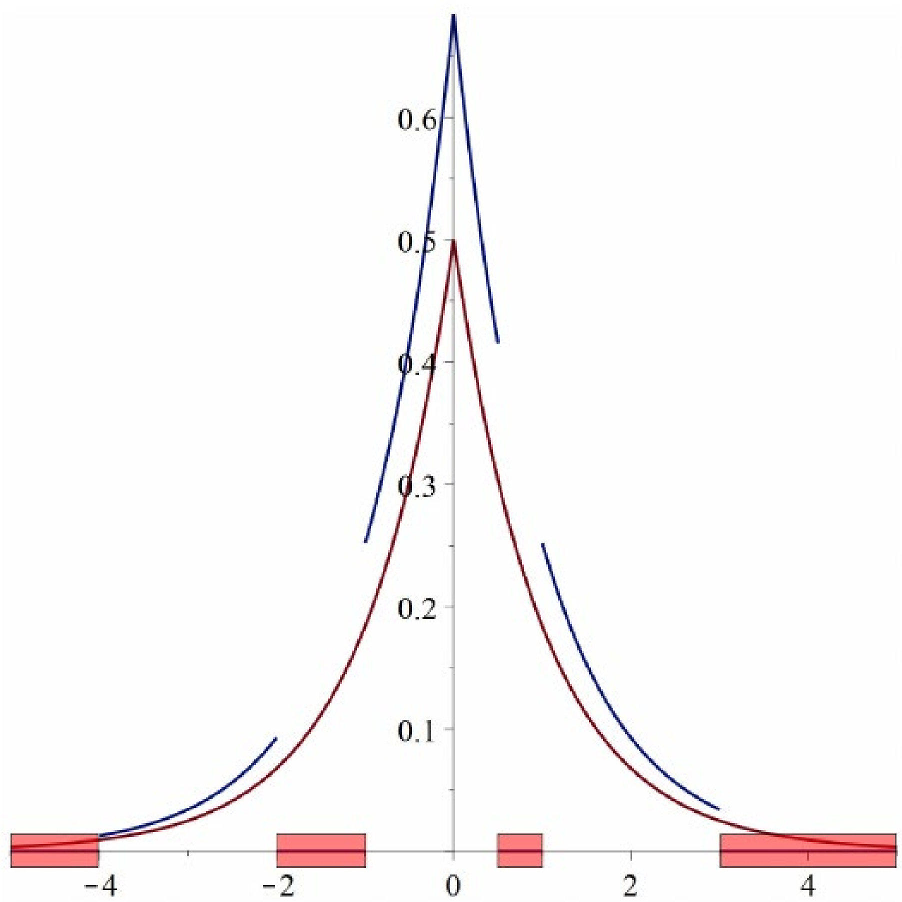
- **Research Problem:**
  - Most differentially private mechanisms add noise with an unbounded range to query responses
  - A lack of adherence to the range of potential true query responses can negatively impact utility

- **Our Work:**
  - We propose new range-adherent mechanisms to improve utility
  - We formally prove adherence of our mechanisms to the differential privacy guarantee
  - We empirically demonstrate improvements in utility over other range-adherent alternatives

Research Method

- **Truncated Distributions:**
  - We propose truncation and normalization of a Laplace distribution to achieve range-adherence
  - We study such distributions within different classes of query range constraints

- **Proposed Mechanisms:**
  - We adapt and apply the differential privacy guarantee to our truncated distributions
  - We calculate optimal scaling parameters for distributions applied to each class of constraints

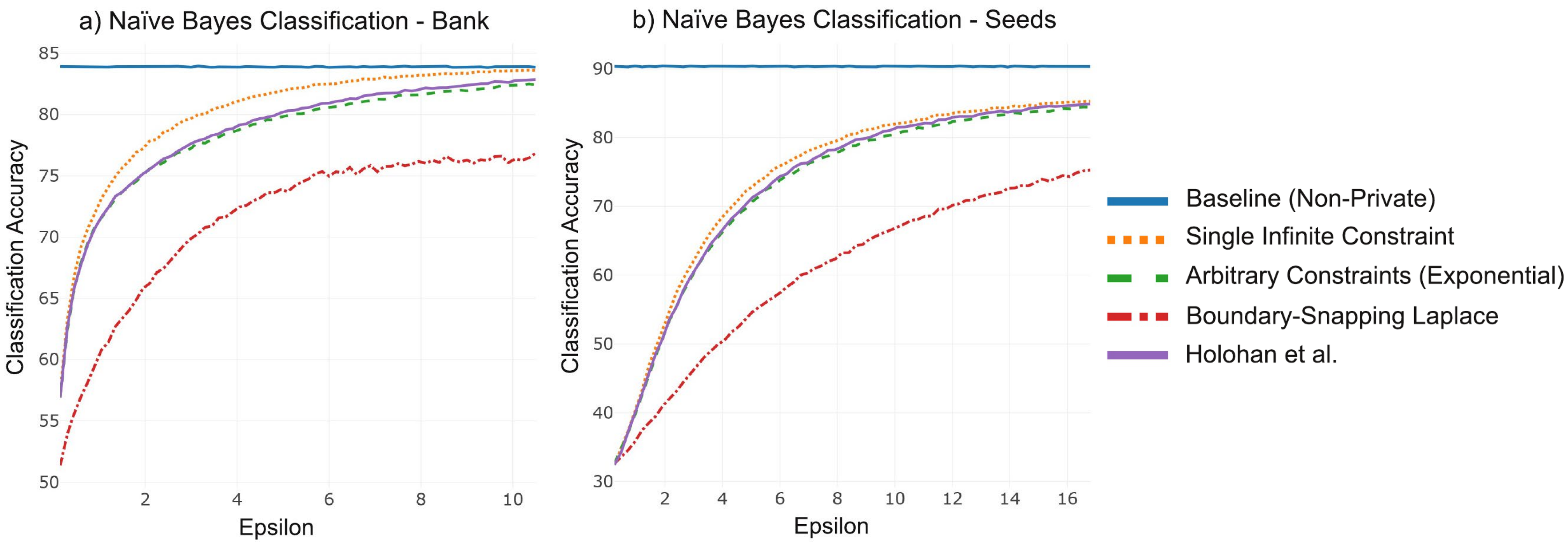


Research Results

- We rigorously prove that each of our proposed mechanisms adhere to the differential privacy guarantee

- We test our mechanisms on the task of differentially private Naïve Bayes classification
  - In particular, standard deviation values must be constrained to remain positive

- Our mechanism for the single infinite constraint setting (orange plot) shows improved classification accuracy over the alternatives



Research Conclusions

- **Contributions:**
  - We provide mechanisms to answer numeric queries in a range-adherent manner
  - We rigorously prove the differential privacy guarantee for all proposed mechanisms
  - We demonstrate improvements in utility over alternative mechanisms

- **Open Problems:**
  - The application of these concepts to relaxations of differential privacy remains an open problem