Differentially Private Aggregation in the Shuffle Model: Almost Central Accuracy in Almost a Single Message[*]

Badih Ghazi[†] Ravi Kumar[†] Pasin Manurangsi[†] Rasmus Pagh[‡] Amer Sinha[†]
[†]Google, Mountain View, CA
[‡]University of Copenhagen, Denmark
{badighazi, ravi.k53, pagh.rasmus}@gmail.com, {pasin, amersinha}@google.com

Summary of Results. The shuffle model of differential privacy has attracted attention in the literature due to it being a middle ground between the well-studied central and local models. In this work, we study the problem of summing (aggregating) real numbers or integers, a basic primitive in numerous machine learning tasks, in the shuffle model. We give a protocol achieving error arbitrarily close to that of the (Discrete) Laplace mechanism in central differential privacy, while each user only sends $1 + o(1)$ short messages in expectation.

[*] The full version of this paper will appear in ICML 2021.