On Mitigating the Utility-Loss in Differentially Private Learning: A New Perspective by a Geometrically Inspired Kernel Approach (Abstract Reprint)

Mohit Kumar[1] , **Bernhard A. Moser**[2,3] and **Lukas Fischer**[3]
[1] University of Rostock
[2] Johannes Kepler University Linz
[3] Software Competence Center Hagenberg GmbH
mohit.kumar@uni-rostock.de, bernhard.moser@scch.at, lukas.fischer@scch.at

Abstract Reprint. This is an abstract reprint of a journal by [Kumar *et al.*, 2024].

Abstract

Privacy-utility tradeoff remains as one of the fundamental issues of differentially private machine learning. This paper introduces a geometrically inspired kernel-based approach to mitigate the accuracy-loss issue in classification. In this approach, a representation of the affine hull of given data points is learned in Reproducing Kernel Hilbert Spaces (RKHS). This leads to a novel distance measure that hides privacy-sensitive information about individual data points and improves the privacy-utility tradeoff via significantly reducing the risk of membership inference attacks. The effectiveness of the approach is demonstrated through experiments on MNIST dataset, Freiburg groceries dataset, and a real biomedical dataset. It is verified that the approach remains computationally practical. The application of the approach to federated learning is considered and it is observed that the accuracy-loss due to data being distributed is either marginal or not significantly high.

References

[Kumar *et al.*, 2024] Mohit Kumar, Bernhard Alois Moser, and Lukas Fischer. On mitigating the utility-loss in differentially private learning: A new perspective by a geometrically inspired kernel approach. *J. Artif. Intell. Res.*, 79:515–567, 2024.