ENCRYPTED COMPUTATIONAL TOPOLOGY

DOMINIC GOLD*, KORAY KARABINA, FRANCIS MOTTA

ABSTRACT. Homomorphic encryption (HE) is a cryptographic primitive which permits, among other operations, both addition and multiplication on encrypted data. Secure end-to-end pipelines, where both the ingested data and output are encrypted to ensure data security and privacy, have been constructed which perform both machine learning (ML) model training and inference on encrypted data. Such data (e.g., genomic, cancer, sensor network, and financial data.), while also sensitive, is often high-dimensional and thus poses practical issues in secure ML tasks.

A burgeoning field of data science known as Topological Data Analaysis (TDA) offers a suite of computational tools that provide quantified shape features in high dimensional data that can be used by modern statistical and predictive ML models. One of the flagship methods, persistent homology (PH), ingests data (e.g., point clouds, images, time series) and derives compact representations of latent topological structures, known as persistence diagrams (PDs). Because PDs enjoy inherent noise tolerance, are interpretable, provide a solid basis for data analysis, and can be made compatible with the expansive set of well-established ML model architectures, PH has been widely adopted for model development, including on the aformentioned sensitive data. For this reason, TDA should be incorporated into the secure end-to-end data analysis pipelines. In this work, we take the first step in developing a version of the fundamental algorithm to compute PH on encrypted data.

Date: May 1, 2023.