zkBoost: Efficient Zero-Knowledge Proofs of Gradient Boosting Training

The rapid development of machine learning has gathered unprecedented attention in the recent years. With these advancements concerns about legitimacy of machine learning have also arisen. Due to its performance, one of the most used techniques in modern machine learning appears to be gradient boosting. To protect the intellectual properties of AI developers, directly examining the training process and data is often prohibited to verifiers.

In response to these challenges we propose a novel zero-knowledge framework for verifying gradient boosting training process. Our framework combines a modernized version of the GKR-protocol with a hidden-order group-based polynomial commitment scheme. By combining these two primitives in a chain-like fashion we were able to achieve time complexity competitive with results for basic training techniques. This particular design avoids being constrained by the sequential nature of machine learning model training process.

Finally, a reference implementation in CUDA is provided, which was tested on a 10-layer 10M-parameters neural network with a batch size of 128. The results show practical applicability of the framework to a life like scenario of training a competitive GPT-based model. To the best of our knowledge this is the first gradient boosting verification framework that is scalable to models with millions of parameters.

Keywords: CRYPTOGRAPHY, MACHINE LEARNING, GRADIENT BOOSTING, ZERO-KNOWLEDGE PROOF, SNARK, COMPLEXITY THEORY, ALGORITHMS