Scalable ZK for ML

Zero-knowledge proofs (ZKPs) are powerful cryptographic techniques that enable a prover to convince a verifier of the validity of a statement without revealing any additional information. Unfortunately, ZKPs typically introduce significant computational overhead compared to performing the native computations directly, which limits the complexity of statements that can be practically proven.

Recently, ZKPs have been explored to verify the correctness and integrity of machine learning (ML) inference. However, current solutions suffer from high computational overhead, mainly due to the expensive evaluation of non-linear functions.

The goal of this thesis is to explore a table lookup approach for efficiently proving non-linear functions in zero-knowledge. The main idea is as follows: the prover (P) and the verifier (V) precompute a public table containing valid input-output pairs for the evaluated non-linear function. Afterwards, P can efficiently prove to V that a given input-output pair exists in the table. Such a table lookup approach can be instantiated using recent techniques developed for ZK proofs of read-only memory (ROM), originally designed to handle verifiable batched memory accesses.

However, a key challenge arises: directly applying table lookups to complex ML functions results in impractically large tables. Therefore, it becomes crucial to carefully design fundamental building blocks such as digital decomposition, comparison, and truncation to enable effective use of smaller tables while maintaining the security and soundness of the proofs. By combining these optimized building blocks, it is possible to implement complex mathematical operations and efficiently construct ZK proofs for mainstream ML non-linear functions, including ReLU, sigmoid, and normalization.

In this project, the student can follow different paths based on their interests and strengths. From a theoretical perspective, the student could focus on applying recent advances in lookup table techniques to this setting. Alternatively, from a practical perspective, the student could implement and evaluate existing approaches across various ML models. This project will introduce the student to cutting-edge research in zero-knowledge proofs and provide valuable insights into privacy-preserving machine learning.

Practicalities

Promoter:	Emmanuela Orsini emmanuela.orsini@unibocconi.it Office 2-C2-03
Nature of the work:	40% literature, 40% theoretical work, 20% software
Number of students:	More than 1
Prerequisites:	A background in cryptography is required and programming skills are recommended