Abstract

Machine learning has seen a great development over the past years, despite the success, there are many serious problems regarding practical cases, one of which is the data privacy concern. A promising approach is to utilize Fully Homomorphic Encryption (FHE) and Zero Knowledge Proof (ZKP) to enable machine learning over encrypted data, however, computing over encrypted data incurs a high computational overhead, thus requiring the redesign of algorithms, in an “ZKP-friendly” manner. This seminar introduces several efficient schemes for ZKP algorithm design, by applying a low degree polynomial approximation for the step function, we realized an efficient protocol for ZK-PPDT tree predictions.