For favour of Posting

Amendment

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

PHD STUDENT SEMINAR

Zero-Knowledge Proofs for Privacy-Preserving Tree Predictions

By

Mr. Zhenhang SHANG

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.

Date : 29 April 2024 (Monday)

Time : 5:30pm

Venue : Room 4503 (Lifts 25-26)

All are Welcome!