The Hong Kong University of Science and Technology

Department of Mathematics

PhD THESIS EXAMINATION

Innovative Protocols for Decentralized Financial Systems and Privacy-Preserving Machine Learning

By

Mr. Zhenhang SHANG

ABSTRACT

This thesis explores the intersection of decentralized finance (DeFi) and privacy-preserving machine learning (PPML) through the design and implementation of novel protocols. The first part of the thesis introduces pvpAMM, a peer-to-peer automated market maker for perpetual contracts, addressing liquidity imbalances in decentralized derivatives markets. The second part focuses on zero-knowledge contingent payments (ZKCP) for decision tree models, enabling fair and private trading of machine learning models. The third part extends this work to privacy-preserving decision tree predictions using fully homomorphic encryption (FHE) and zero-knowledge proofs (ZKP). Together, these contributions advance the fields of DeFi and PPML by providing scalable, secure, and privacy-preserving solutions for financial and machine learning applications.

Date : 24 October 2025, Friday

Time : 2:00 pm

Venue : Room 4472 (Lifts 25/26)

***Thesis Examination Committee*:**

Chairman	**:**	**Prof. Cunsheng DING, CSE/HKUST**
Thesis Supervisor	**:**	**Prof. Kani CHEN, MATH/HKUST**
Member	**:**	**Prof. Beifang CHEN, MATH/HKUST**
Member	**:**	**Prof. Lixin WU, MATH/HKUST**
Member	**:**	**Prof. Yangqiu SONG, CSE/HKUST**
External Examiner	**:**	**Prof. Weili HAN, School of Software/ Fudan University** *(via online mode)*

(Open to all faculty and students)

The student's thesis is now being displayed on the reception counter in the General Administration Office (Room 3461).