University of Pittsburgh | School of Computing and Information

Dissertation Defense

Doctor of Philosophy in Information Science

"Defense Mechanisms for Economic Attacks in Blockchain-based Decentralized Finance (DeFi)"
by Abdulrahman Alhaidari

Date: November 20, 2026
Time: 10 a.m. – Noon
Place: Room 828, Information Sciences Building, 135 N. Bellefield Ave, Pittsburgh PA 15260

Committee:

- Balaji Palanisamy, Associate Professor and Advisor, Department of Informatics and Networked Systems, School of Computing and Information
- Prashant Krishnamurthy, Professor, Department of Informatics and Networked Systems, School of Computing and Information
- Pengfei Zhou, Assistant Professor, Department of Informatics and Networked Systems, School of Computing and Information
- Xulong Tang, Associate Professor, Department of Computer Science, School of Computing and Information

Abstract:

Blockchains power decentralized finance (DeFi) protocols for lending, borrowing, and trading without centralized intermediaries. DeFi protocols hold billions in Total Value Locked (TVL), which makes them targets for economic attacks that drain tokens, vaults, and liquidity pools. Losses persist despite audits, formal verification, and static analysis because they check whether code behaves as written, but not whether funds can leave the protocol without authorization. A contract that passes code-level checks can still lose funds because not all attacks require a code flaw. Correct contracts can become exploitable when composed. When a flaw exists, the protocol's economic state, including balances and reserves, can determine its exploitability. This dissertation presents detection and defense mechanisms against unauthorized fund exits.

The dissertation makes five contributions, each evaluated on real economic exploits. First, it introduces FlashGuard, a runtime defense for Ethereum Virtual Machine (EVM) blockchains that mitigates non-price flash loan attacks, which prime the protocol's economic state before an exploit. A dusting counterattack alters the victim contract's state and forces the attack to revert. Second, since FlashGuard covers one attack class in the public mempool, the dissertation develops a decentralized on-chain learning, governance, and inference framework that detects multiple attack classes regardless of the submission channel, including private relays. On-chain machine-learning models run as smart contracts under bounded gas and bit-exact constraints, and a Proof-of-Improvement (PoIm) protocol accepts only updates that improve detection.

Third, because on-chain machine-learning detection learns from static attributes of observed attacks, it does not transfer to unseen exploits. TxAnchor is a zero-shot detection framework that models the realized economic effect of an attack transaction. It recovers held-out exploit families

and transfers to unseen chains and a later period without retraining. Fourth, TIDES (Temporal Inference of DeFi Exploitability States) formalizes state-conditioned exploitability and reveals when the state permits a vulnerability to become exploitable. Most exploits measured across seven EVM blockchains require a favorable economic state, and vulnerable code alone is not sufficient. Finally, Guarding-the-Exit (GTE) is a vulnerability-agnostic framework that synthesizes the exit paths that drain funds when contracts compose at runtime. Overall, the dissertation establishes a fund-exit-path-oriented foundation for securing DeFi against state-dependent economic exploits.