University of Pittsburgh | School of Computing and Information

Dissertation Defense

Masters in Computer Science

“**Privacy-Preserving Phragmén’s Elections for Nominated Proof-of-Stake (NPoS) Blockchain Systems**” by **Purva Chaudhari**

Date:	Aug. 4, 2025
Time:	3:00 – 5:00 p.m.
Place:	6143 Sennott Square, 3810 Forbes Ave, Pittsburgh, PA 15260

Committee:

- Dr. Adam Lee, Dissertation Co-Chair, Dept of Computer Science, School of Computing and Information
- Dr. Balaji Palanisamy, Dissertation Co-Chair, Department of Informatics & Networked Systems, School of Computing and Information
- Dr. Stephen Lee, Dept of Computer Science, School of Computing and Information

Abstract:

Blockchain networks increasingly rely on decentralized, stake-based governance to maintain security, fairness, and community trust. Among these, Polkadot’s Nominated Proof-of-Stake (NPoS) system stands out by leveraging sequential Phragmén’s method to select a validator set that fairly represents nominators' preferences and stake contributions. While this approach effectively balances decentralization and stake-weighted influence, it operates with full transparency: all nomination preferences, stake distributions, and intermediate election states are publicly visible on-chain. This openness, though essential for auditability, introduces critical privacy risks—enabling strategic manipulation, coercion, and vote buying.

In this thesis, we present the first tally-hiding implementation of sequential Phragmén’s election using secure multiparty computation (MPC). Our approach allows validator sets to be computed entirely over encrypted data, revealing only the final election outcome while keeping all intermediate votes, stake contributions, and approval patterns confidential. We extend the existing Ordinos framework by designing novel MPC primitives, including secure encrypted fractional division and iterative load updates essential for stake-weighted proportionality. We formalize an encrypted bipartite graph representation of nominators and validators, supporting encrypted score computation and dynamic load balancing. Our experimental evaluation on synthetic election datasets demonstrates that our tally-hiding protocol achieves near-ideal stake distribution accuracy with practical runtime overheads. This work bridges a critical gap in blockchain governance by enabling private, verifiable, and fair validator elections, offering a concrete path toward privacy-preserving on-chain governance systems that reconcile openness with individual confidentiality.