Improving Bitcoin's Post-Quantum Transaction Efficiency With a Novel Lattice-Based Aggregate Signature Scheme Based on CRYSTALS-Dilithium and a STARK Protocol

Quan, Yunjia (School: Charlotte Country Day School)

Quantum computing is revolutionizing cryptography, as it will render the classical digital signature schemes such as Bitcoin's ECDSA (Elliptic Curve Digital Signature Algorithm) insecure. Thus, quantum-resistant (post-quantum) signature schemes are developed to protect Bitcoin. However, the large signature sizes of these existing post-quantum schemes will cause Bitcoin's post-quantum transaction efficiency to significantly decrease, which will be detrimental to the $542 billion Bitcoin market. In this research, a novel lattice-based aggregate signature (LAS) scheme is crafted to improve Bitcoin's post-quantum transaction efficiency by generating small signatures. It is used with a Scalable Transparent Arguments of Knowledge (STARK) protocol, which generates a zero-knowledge proof with each signature to protect traders' privacy. With compactness, correctness, and unforgeability proofs, the proposed scheme demonstrates Strong Unforgeability under Chosen Message Attacks in the Quantum Random Oracle Model. The scheme also has the following advantages: easy implementation due to the use of Number Theoretic Transform, unordered aggregation, and the elimination of rogue attacks. Implemented in Python, the proposed LAS scheme surpassed existing post-quantum schemes in transaction efficiency: the proposed scheme is six times more efficient than CRYSTALS-Dilithium, the primary post-quantum signature scheme selected by the National Institute of Standards and Technology, and more efficient than four other LAS schemes. This efficiency improvement is crucial for post-quantum Bitcoin, and the proposed scheme also allows for more security, sustainability, protection of privacy, and easy implementation.

Awards Won:

Third Award of $1,000

American Mathematical Society: Honorable Mention and One-Year Membership to AMS (for 5 projects with up to 3 team members per project)