Exploring the Use of Hybrid Post-Quantum Key Exchange in TLS 1.3

Wang, Alexander (School: Kalani High School)

This project investigates the feasibility of integrating hybrid post-quantum key exchange into TLS 1.3 by combining classical elliptic-curve cryptography (X25519) with a post-quantum key exchange (ML-KEM-768). As quantum computing poses a future threat to current cryptographic methods, this research evaluates the performance impact of classical, post-quantum, and hybrid key exchange on TLS 1.3 handshake latency under identical system and network conditions. TLS 1.3 handshakes were implemented using OpenSSL on controlled local network systems, and latency was measured across repeated automated trials to ensure consistency. The study benchmarks key exchange performance at two levels: Part A measures algorithm-level computation speed, and Part B measures end-to-end TLS handshake time. In Part B, across 300 handshake trials per configuration, mean handshake times were 3.856 ms (X25519), 4.059 ms (ML-KEM-768), and 4.243 ms (hybrid), corresponding to +5.25% (ML-KEM-768) and +10.02% (hybrid) increases over the classical baseline. These results suggest hybrid key exchange can serve as a practical transition path toward quantum-safe TLS with a measurable but manageable latency overhead, supporting deployment in real-world systems while maintaining performance viability.

Awards Won:
Association for the Advancement of Artificial Intelligence: AAAI Student Memberships for each finalist that is part of the 1st, 2nd, and 3rd Prize Winning projects and 5 Honorable Mention winning projects (up to 3 students per project) (in-kind award / part of the 1st-3rd prize)