Title: Replacing Public Cryptographic Key Exchanges with Quantum Resistant Implementations: The Future of VPN and Enterprise Network Security

Presenter: Adam Ismail, Pasadena City College
Mentor: Jared Ashcroft

Modern networking equipment relies on exchange of public keys to establish secure sessions or tunnels, like VPNs or HTTPS websites. Cryptographic functions are vulnerable to quantum computations. Classic Diffie–Hellman key exchange (MODP) revolves around discrete logarithm problems which state it is difficult to extract private keys a and b from [g^(ab)]mod(p)]. This algorithm has been broken without quantum computations, and a shift was made to elliptic curve based Diffie–Hellman exchanges (ECDH). Elliptic curves are abstract algebraic structures called abelian groups. An example of secure elliptic curve formula is y^2 = x^3+486662x^2+x(mod(2^255 - 19)), where we solve for a new point [private key]xP, where P is a given arbitrary point on the curve. Addition in abelian groups across a modulus operator yields discrete mapping of the curve, and this mapping seems utterly random if discovered by a man-in-the-middle, just as how the private key is obfuscated using modular arithmetic in MODP problem. ECDH needs the shortest keys, which makes it easiest for a quantum computer to crack. The only choice is to use quantum-resistant methods with more abstract bases. Another implementation of elliptic curves relies on a pool of curves, and creating random paths between them. Using elliptic curves, already been studied and implemented widely on modern routers and firewall devices, would be more straightforward for vendors to issue updates that adapt founded mechanics to more sophisticated encryptions. This supersingular isogeny elliptic curve Diffie–Hellman (SIDH) would be a legitimately quantum-resistant algorithm, but has yet to see official implementation in devices.