1176-68-133 **Reza Azarderakhsh*** (razarderakhsh@fau.edu), 777 Glades Rd, EE313, Boca Raton, FL 33431. *Practical Post-Quantum Cryptography Based on Isogenies on Supersingular Curves.*

It has been widely accepted that quantum computer attacks on today's security are expected to become a reality within the next decade. Some progress towards constructing quantum computers has been made, although no quantum computers with serious computing power have yet been built. Nevertheless, we believe it is prudent to plan for future needs as it normally takes many years to change cryptosystem deployments. Furthermore, due to network effects and existing schemes with the perfect forward secrecy property, today's cryptosystems will remain vulnerable as attackers can record encrypted data now and decrypt in the future when quantum computers become available. In this presentation, I will talk about quantum-safe solutions, including post-quantum primitives, encryption algorithms and key exchange mechanisms, that we are currently involved and are feasible to be implemented in small and resource-constrained devices. I mainly will discuss the efficiency of implementing isogeny-based cryptography, which are based on hardness of finding maps between elliptic curves, on different hardware platforms and provide the timing and performance results in widely used IoT devices. (Received January 18, 2022)