Design, Implementation, and Analysis of Quantum-Resistant Algorithms on Smart Handheld Embedded Devices

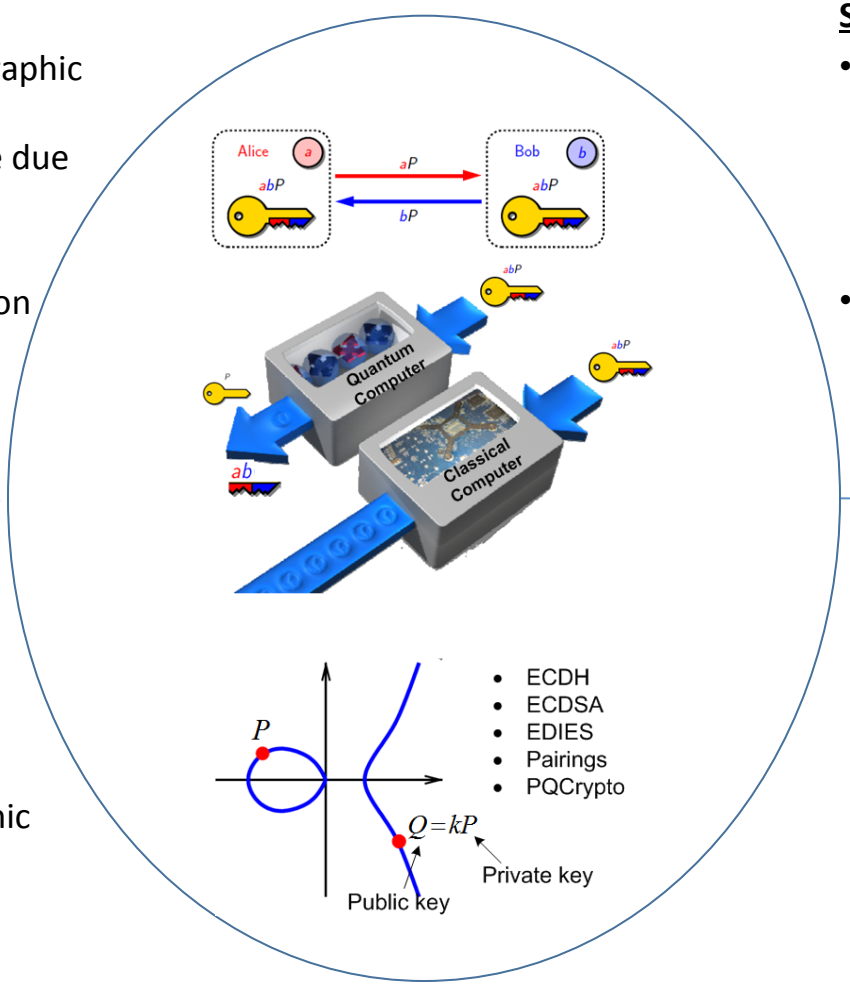
FAU
FLORIDA ATLANTIC UNIVERSITY

Challenge:

- The current classical cryptographic algorithms for public key cryptography will be insecure due to the presence of quantum computers.
- Post-quantum cryptography on embedded devices

Solution:

- Isogenies on supersingular elliptic curves
- a bottom-up approach and study the use of new families of isogenies in designing, implementing, and analyzing new and existing cryptographic protocols
- Smallest key size
- Perfect forward secrecy
- 32-, 64-bit ARM implementations



Scientific Impact:

- Providing practical solutions for ensuring security in the presence of quantum computers on Embedded devices.
- the goal here is to develop quantum-resistant cryptosystems in anticipation of quantum computers.

Broader Impact:

- Making internet secure against quantum computers.
- FUA: Cryptographic Engineering course developed, PQCrypt, CHES, AsiaPKC. Teaching undergrad courses. Female and minorities involved.

NSF-CRII 1661557, Florida Atlantic University, PI: Reza Azarderakhsh, razarderakhsh@fau.edu

To be cyber-safe we must be quantum-safe.