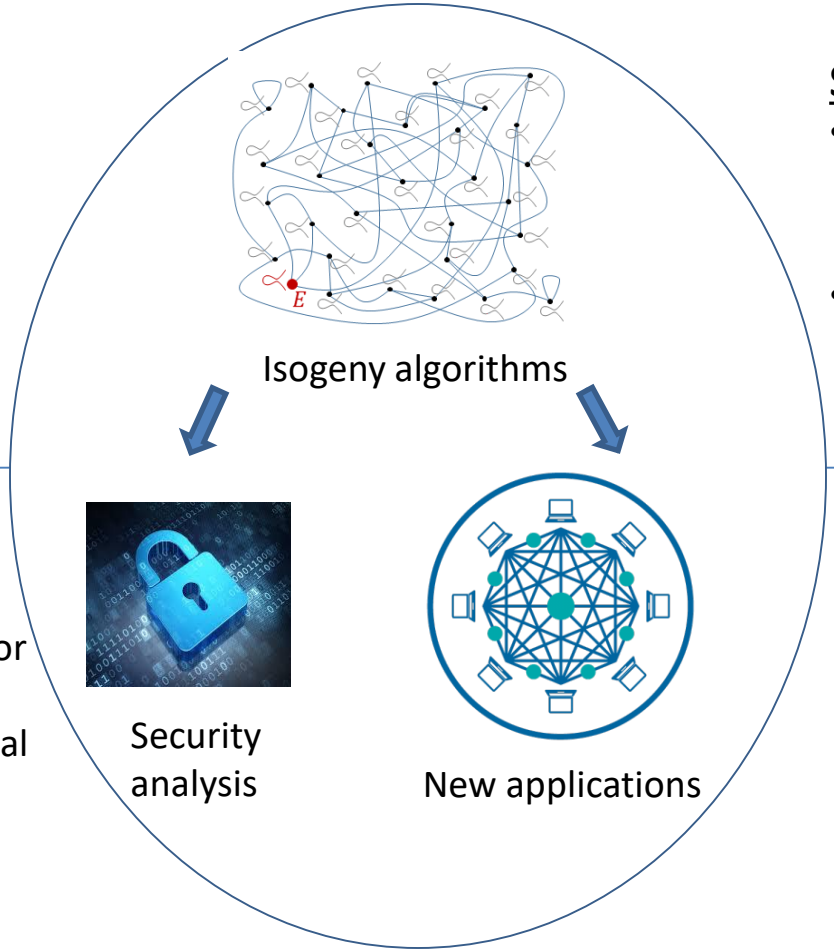
EAGER: Quantum-Safe Cryptosystems Based on Isogenies

Challenge:

- Analysis of security of isogeny-based crypto schemes
- Creation of new functionalities for isogeny-based crypto schemes

Solution:

- Description of new quantum algorithms for attacks.
- Leverage mathematical structure for new functionalities.



Scientific Impact:

- The project provides a better understanding of the security of isogeny-based schemes.
- Isogeny-based systems are one of the very few proposals for quantum-safe cryptography.

Broader Impact:

- New cryptography needs to be standardized and deployed. In particular, NIST needs input for this task.
- Transition to practice includes refinement of the key sizes for the NIST candidates.
- Outreach: cybersecurity summer camps

- Award number 1839805
- University of South Florida

- Contact: biasse@usf.edu