Algorithms for number-theoretic problems in cryptography

Challenges:

Quantum computers can break many cryptosystems:

RSA, discrete-log based cryptosystems, Buchmann-Williams key exchange, Soliloquy, multilinear map-based encryption and Smart-Vercauteren fully homomorphic encryption scheme.

We have to establish which proposed replacements for these systems - if any - are secure against quantum computers before they are built.

Other challenge: make existing classical curve-based cryptosystems more efficient.

Solution:

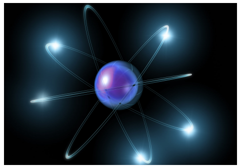
Study some recently proposed systems and determine if they are secure again quantum computers. Possible replacements for currently used cryptosystems include:

- Encryption scheme based on supersingular elliptic curve isogenies. So far this system is secure classically and against quantum computers.
- Lattice-based systems. One possibility to break these systems: extend algorithm for computing the unit group of a number field that broke several lattice-based systems.

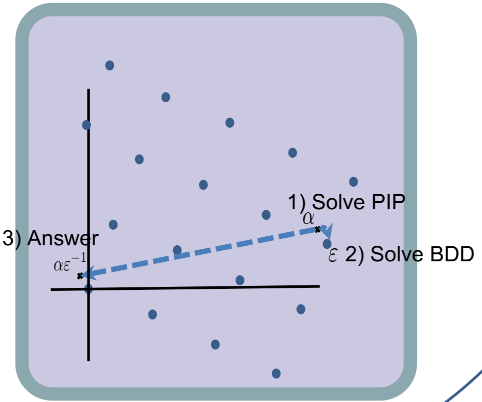
NSF award number: CNS 1617802

PI: Kirsten Eisentraeger, Penn State University, eisentra@math.psu.edu

Co-PI: Sean Hallgren, Penn State University, hallgren@cse.psu.edu



Breaking cryptosystems with quantum computers



Scientific Impact:

- Increase confidence in the security of cryptosystems which will replace current ones.
- Determine which proposed cryptosystems are insecure against quantum computers.
- Determine how to make currently used curve-based systems more efficient. Important for small devices like cell phones.

Broader Impact:

- Impact on national security: confidential information has to remain secure indefinitely even if quantum computers are built in the near future.
- Effect on e-commerce and other areas with confidential data like healthcare: only cryptosystems that are secure against quantum computers should be recommended for use in e-commerce or to access confidential data.
- PI will run a workshop for Women in Number Theory on these topics at a conference in Banff (August 2017).