Classical and quantum algorithms for number-theoretic problems arising in cryptography

Challenges:

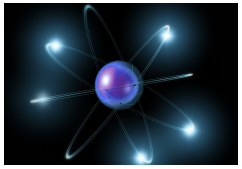
Quantum computers can break many cryptosystems:

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

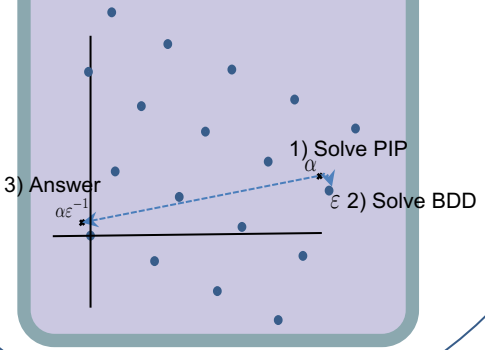
We need to establish which proposed replacements for these systems - if any - are secure against quantum computers before they are built.

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

Solution: Study recently proposed systems and determine if they are secure against quantum computers. Study underlying hardness assumptions and find reductions to other problems.



Breaking cryptosystems with quantum computers



Progress so far:

- For encryption schemes based on supersingular elliptic curve isogenies: Showed that security of all systems reduces to hardness of endomorphism ring problem. We gave a new classical algorithm for this problem that is faster than previous ones. So far, our algorithm is still exponential. Next step is to look for a quantum algorithm.
- Lattice-based systems are often based on hardness of Bounded Distance Decoding (BDD). We gave a new quantum algorithm for BDD, that is efficient for a new range of approximation factors.

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 and co-PI are designing a webpage with current state of the art in lattice-based cryptography and are soliciting input from researchers in the community.

NSF award number: CNS 2001470

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

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