Algorithms for number-theoretic problems in cryptography

PIs: Kirsten Eisentraeger and Sean Hallgren, Penn State University

Challenges and Goals:

Challenge: Quantum algorithms can break RSA, discrete-log based cryptosystems, Buchmann-Williams key exchange, Soliloquy, the Smart-Vercauteren fully homomorphic encryption scheme and multilinear map-based encryption. We have to establish which proposed replacements are secure against them before quantum computers are built.

Possible alternatives to RSA and Elliptic Curve crypto:

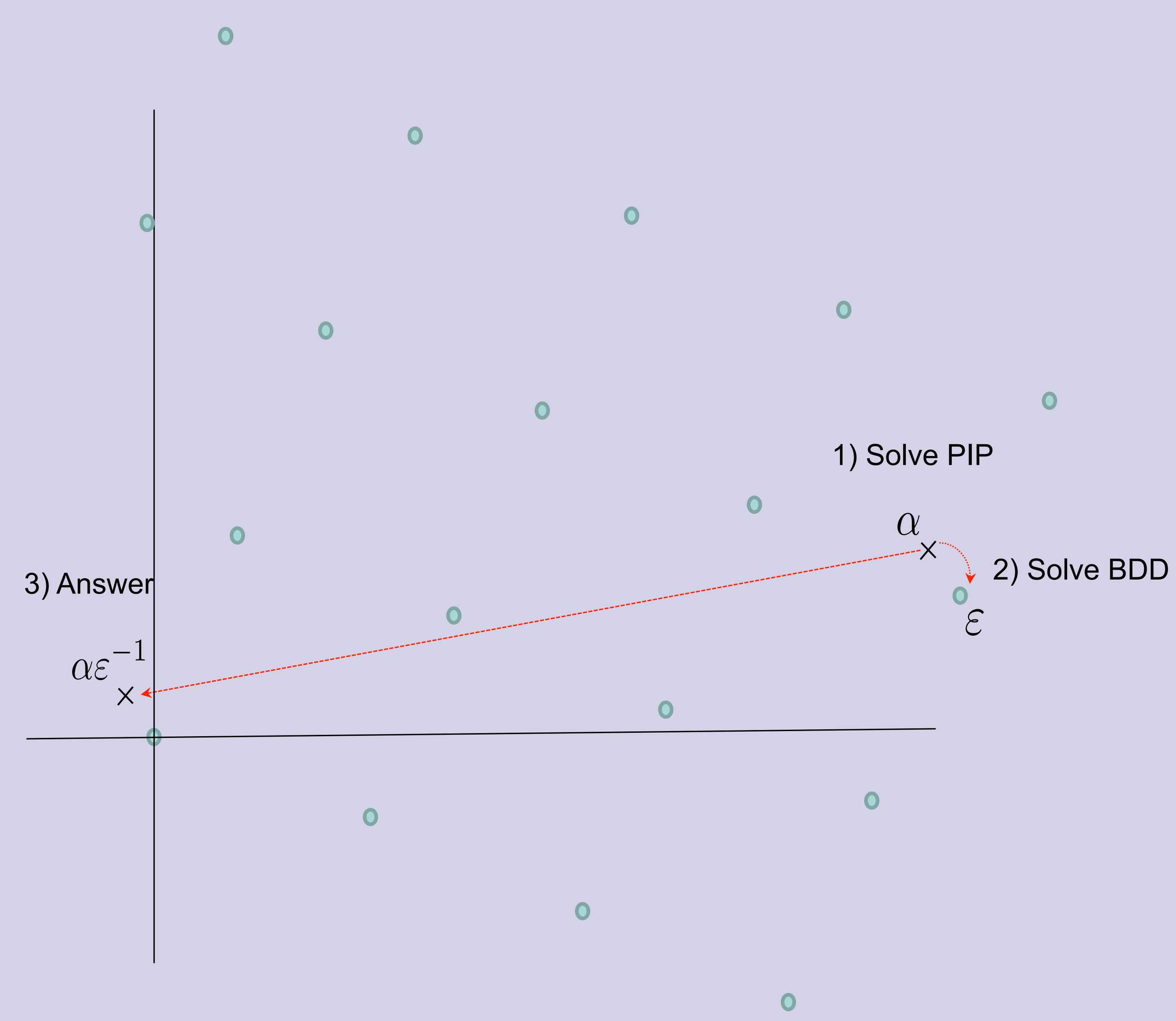
1. Lattice-based systems (e.g. systems based on Ring-LWE)
2. System based on isogenies between supersingular elliptic curves

Goals of this project:

1. Study and determine the security of these recently proposed systems.
2. Make curve-based classical systems more efficient.

Lattice-based systems:
Advantages: have fully homomorphic encryption schemes based on Ring-LWE.
Applications: predictive analysis, genomic computations and many others.
Underlying hardness assumptions: finding shortest vectors or computing short generators or solving Bounded Distance Decoding in ideal lattices is hard.

Computing a short generator of a principal ideal



Approach to breaking lattice-based systems

- Take the underlying hardness assumption and express it in terms of a well known lattice problem (e.g. shortest vector problem, Bounded Distance Decoding - BDD).
- First approach: try to break special instances of the system directly (e.g. for Ring-LWE).
- Second approach: solve the underlying lattice problem with a generalization of the unit group algorithm by Eisentraeger-Hallgren-Kitaev-Song.

Breaking Soliloquy

Soliloquy was developed by GCHQ as a post-quantum public-key cryptosystem.

Public key: basis for an ideal in a cyclotomic number field that is known to have a short generator

Secret key: the short generator of the principal ideal

Attacking the system works in two steps:
(1) Use the unit group algorithm of Hallgren-Eisentraeger-Kitaev-Song together with an extension by Biasse-Song to find *some* generator α of the ideal.
(2) Convert the generator to a *short* generator. This recovers the secret key.

Breaking other lattice-based systems?

Questions:

- Step (1) in the Soliloquy attacks works for any number field. Can Step (2) be extended to more general number fields to attack more lattice-based systems?
- Is it possible to give specific conditions on the basis of the unit lattice of a given number field that will imply that Babai's rounding algorithm can solve Bounded Distance Decoding problem in this lattice?
- First approach: try approach on large subfields of cyclotomic number fields.

Cryptosystems from supersingular elliptic curve isogenies

So far: promising candidate for post-quantum secure system.

Underlying ring is non-commutative, so have to publish auxiliary points on the curve in the protocol.

Questions:
1. How to use auxiliary points to attack the system directly?
2. Are there standard elliptic curve invariants (e.g. endomorphism ring) that can be computed with a quantum computer that can be used to break the system?

Approach for attack on supersingular isogeny cryptosystems

Secret key: certain isogeny (map) on the elliptic curve

Idea for attack: Step 1. Solve analogous problem for quaternion algebras using Kohel-Lauter-Petit-Tignol.

Step 2. Use one-to-one correspondence between supersingular elliptic curves and certain quaternion algebras to recover secret isogeny. Relate supersingular curves and quaternion algebras through endomorphism ring. **Open** how to compute the endomorphism ring efficiently.

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting

National Science Foundation
WHERE DISCOVERIES BEGIN

PennState
Eberly College of Science