CAREER: Algebraic Methods for the Computation of Approximate Short Vectors in Ideal Lattices

Challenge:

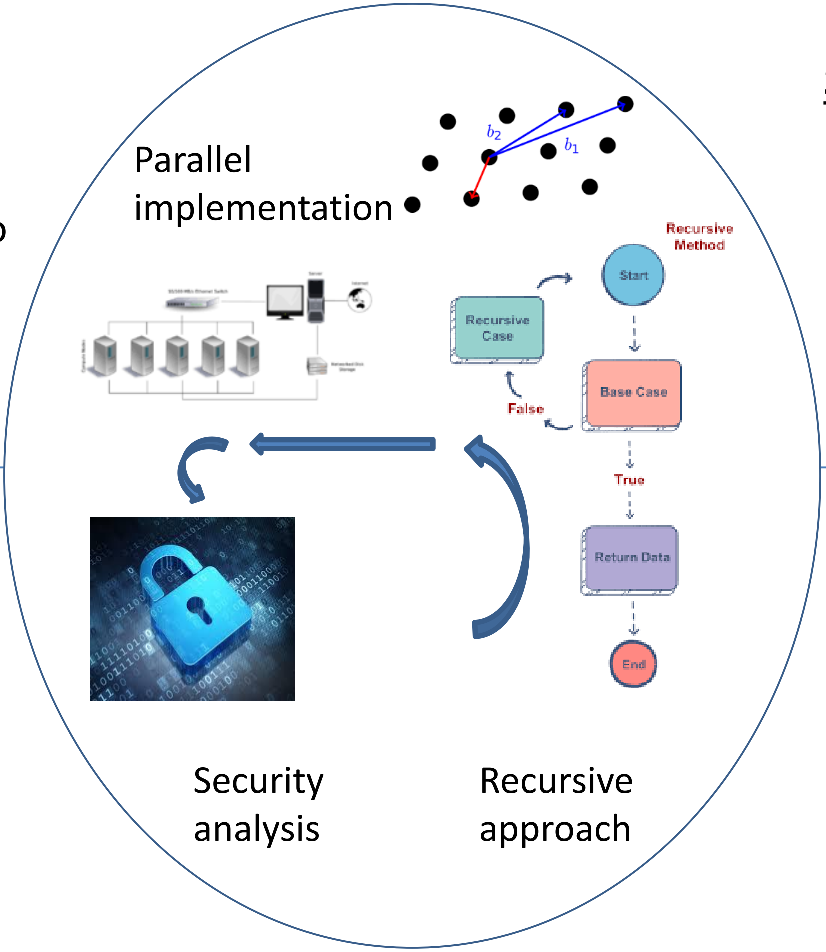
1. Analysis of security of ideal lattice-based crypto schemes

2. Understanding the hardness of finding short vectors in ideal lattices

Solution:

- Description of a new recursive algorithm.
- Implementation and study of the practical performances.

- Award number 1846166
- University of South Florida
- Contact: biasse@usf.edu



Parallel implementation

Security analysis

Recursive approach

Scientific Impact:

- The project provides a better understanding of the security of lattice-based schemes.
- Lattice-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