TEXAS
The University of Texas at Austin

SaTC: CORE: Small: Expanding the Frontiers of Lattice-Based Cryptography

Challenge:

- Large-scale quantum computers would compromise many of the cryptographic protocols currently in use today
- Post-quantum constructions of advanced cryptographic primitives often have high overhead compared to their pre-quantum analogs

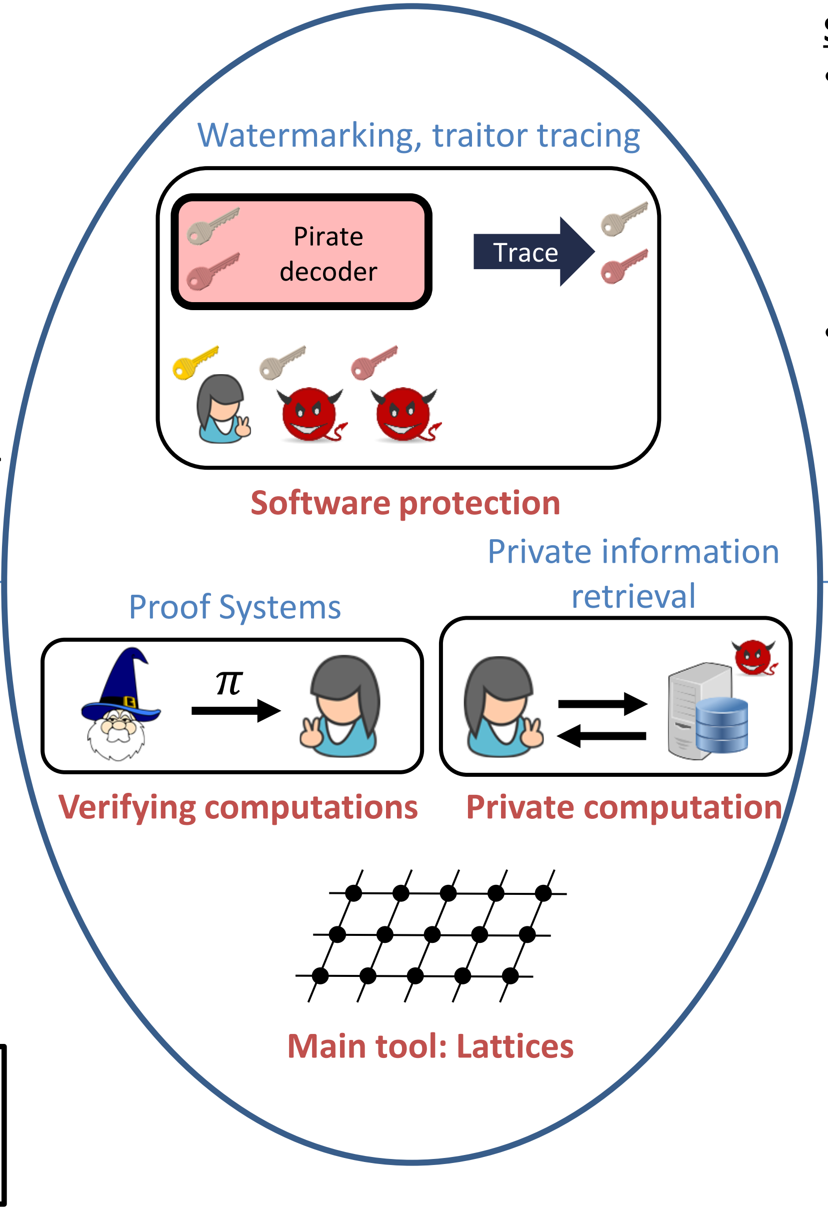
Solution:

- Lattice-based cryptography provides a sound foundation for realizing post-quantum cryptography
- This project studies new techniques and frameworks for constructing lattice-based cryptographic primitives for protecting computations and software and for verifying the integrity of computations

Award Number: NSF CNS-2151131

Institution: UT Austin

PI: David Wu



Watermarking, traitor tracing

Software protection

Proof Systems

Verifying computations

Private information retrieval

Private computation

Main tool: Lattices

Scientific Impact:

- Expands the scope and capabilities of lattice-based cryptography through new constructions of proof systems, watermarking, and traitor tracing
- Introduced new and concretely-efficient realizations of lattice-based proof systems and private information retrieval (PIR)

Broader Impact and Broader Participation:

- Open-source implementations of lattice-based protocols (zkSNARKs and private information retrieval)
- Developed new course on lattice-based cryptography – goal will be to have a set of public lecture notes synthesizing major developments from last 10 years
- Has supported and continue to support multiple PhD, MS, and undergraduate student research projects