Cryptographic Hardness of Module Lattices

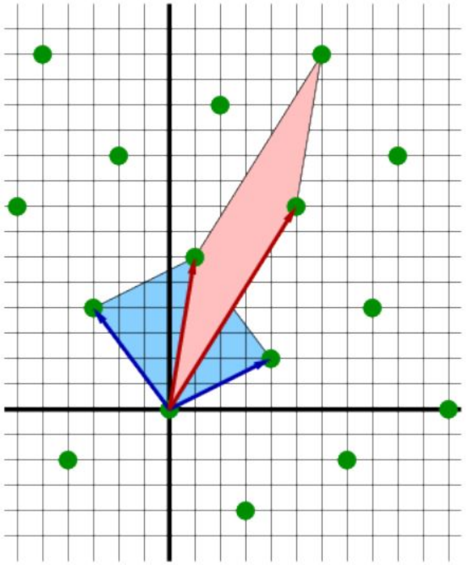
Challenge:

- Structured lattices provide versatile and powerful constructions in lattice-based cryptography;
- Central to the security evaluation for the current NIST competition;
- Lack of clear understanding on the intractability of structured lattice problems.

-

Solution:

- Investigating if there is a hardness gap between SIVP for rank-1 modules (i.e., ideal-SVP) and rank-2 modules;
- Finding the relation of NTRU compared to other module lattice problems.
- Assessing whether module-SIVP in rank ≥ 2 is easier to solve than SIVP for arbitrary lattices of the same dimension and investigating more efficient algorithms for module-SIVP.



NSF #2122229:

Shi Bai, Florida Atlantic University.
Noah Stephens-Davidowitz, Cornell University.

Scientific Impact:

- The research findings benefit the cryptography community and developers of lattice-based cryptosystems;
- Informing the current cryptographic standard process by NIST by suggesting better parameters;
- Improving cryptographic standards and cryptographic efficiency.

Broader Impact and Broader Participation:

- Contribute to the training of STEM workforce in cybersecurity;
- Strengthening the participation of under-represented groups;
- Disseminating the results to the general audience;
- Integrated research and education.