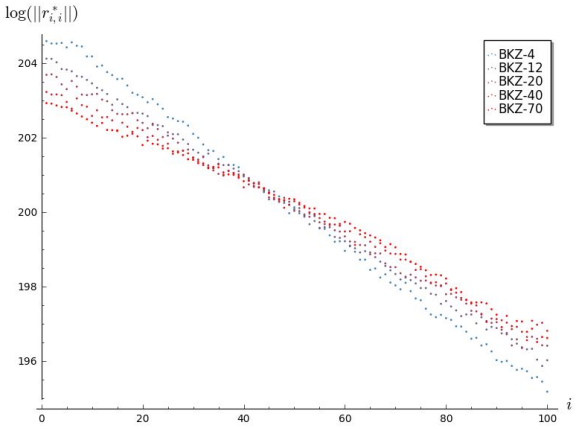
CAREER: Concrete Hardness in Lattice-based Cryptography

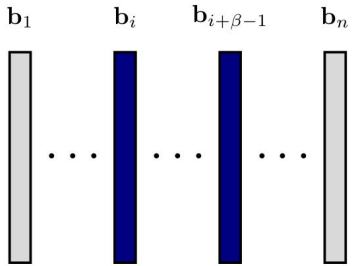
Challenge:

* Concrete security of lattice-based assumptions is not fully understood.
* Several complexity models are being used, sometime contradicting.
* Need to derive the crossover point between lattice sieving and enumeration for cryptographic relevant parameters.



Solution:

* Investigate better lattice reduction strategies.
* Improve enumeration-based lattice reduction algorithms.
* Explore memory-efficient sieving variants.
* More precise quantum resource estimate for lattice reduction.



$$\|\mathbf{b}_i^*\| = \|\mathbf{b}_i^{(i)}\| = \lambda_1\left(\mathcal{L}\left(\mathbf{b}_i^{(i)}, \mathbf{b}_{i+1}^{(i)}, \cdots, \mathbf{b}_{\min(i+\beta-1,n)}^{(i)}\right)\right), \ \forall 1 \le i \le n$$

NSF #2044855:
Shi Bai, Florida Atlantic University.

Scientific Impact:

* Benefit the cryptography community, developers of lattice-based cryptosystems, and ordinary users of post-quantum cryptographic products.
* Provide guidance on how to choose appropriate parameters to meet specific security levels.

Broader Impact and Broader Participation:

* Student involvement in research and contribution to cybersecurity workforce.
* Education Initiatives addressing underrepresented groups and minority students
* Outreach and science communication events such as crypto summer camps.