Short vectors in lattices (1913167, 1913210)

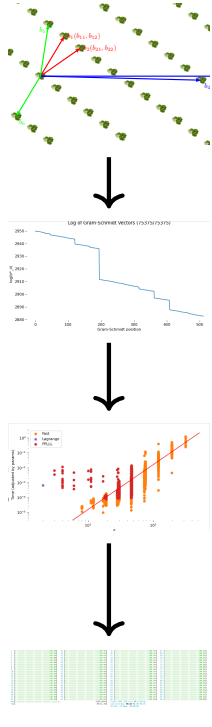
Challenge:

- Design, implement, and test a fully parallelized and more efficient lattice basis reduction algorithm.
- Exploit ideal lattices.

Solution:

- Characterize the properties of classes of lattices that are important for applications. (Done.)
- Design new algorithm with fastest proven runtime. (90% completed.)
- Implement and benchmark new algorithm. (In progress.)
- New S-unit attacks for ideal lattices. (Code released.)

Daniel J. Bernstein	UIC
Nadia Heninger	UCSD



Scientific impact:

- Improved understanding of these algorithms, in theory and in practice.
- Connections to supercomputing.
- Connections to algebraic number theory.
- New open-source software for these algorithms.

Broader impact and broader participation:

- Many post-quantum proposals rely on difficulty of lattice problems.
- Widespread deployment seems likely.
- Algorithm development is critical for avoiding weak cryptographic systems.
- Training PhD student: Keegan Ryan, UCSD.