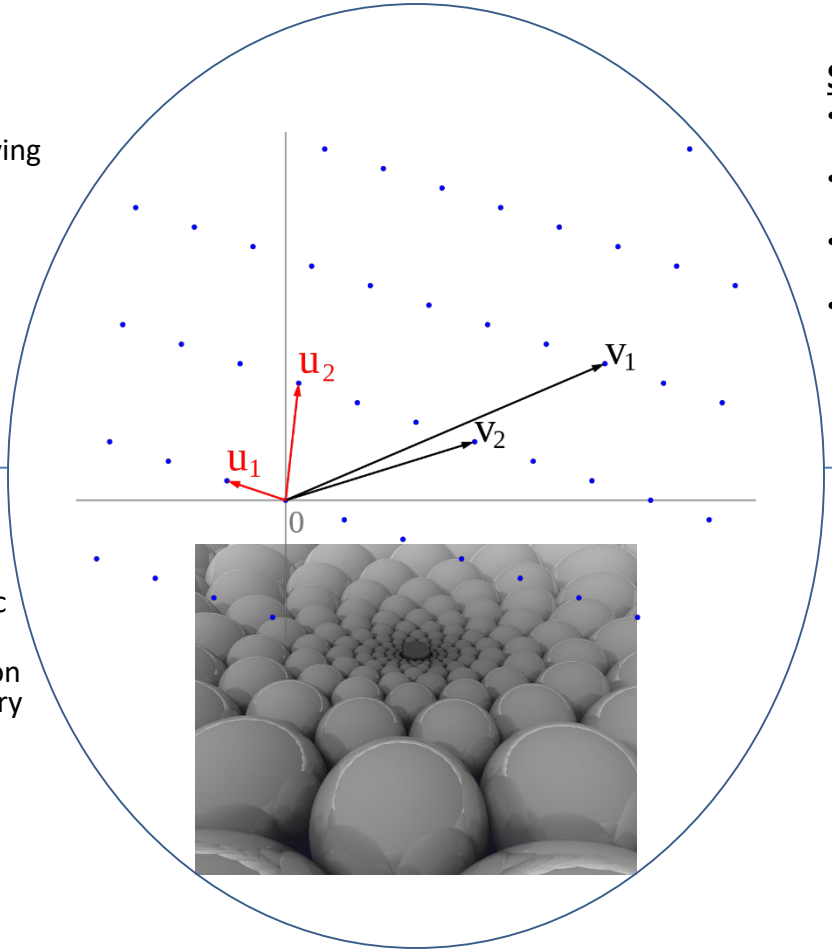
Lattices, number theory, and distribution questions in cryptography

Challenge:

- Understand difficult underlying mathematics of new lattice-based cryptosystems
- How secure are lattice basis generation algorithms?



Scientific Impact:

- New understanding of lattice shapes
- Machinery to improve security estimates
- Distribution of side-channel information
- Found weakness in DRS post-quantum NIST submision

Solution:

- Introduce methods from number theory ("automorphic forms")
- Analyze lattice basis generation from viewpoint of group theory
- Normalized histograms of timing information

Broader Impact:

- Studies potential threats to current cryptosystems
- Parameters for post-quantum crypto
- Bringing mathematicians together with cryptographers to learn where math can have the greatest impact

SaTC-Small grant CNS-2124692 , Rutgers University (PI: Stephen D. Miller)