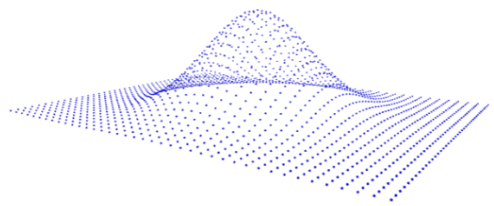
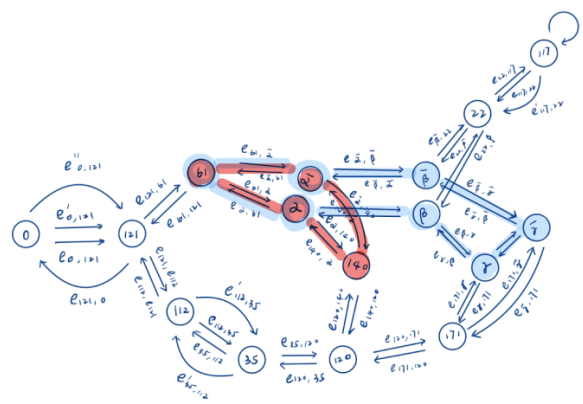
CAREER:
Research and Education: Number Theory, Geometry and Cryptography

University of Colorado Boulder

Challenge:

- The mathematical underpinnings of post-quantum cryptography need to be analysed for their security.





Images due to Katherine E. Stange and Mingjie Chen

Scientific Impact:

- Develop trust in new crytographic assumptions.
- Advance the understanding of the limits of secure parameters.

Solution:

- Mathematical research into underlying hard problems.
- Improved Ring-LWE and isogeny-based attacks.

Broader Impact and Broader Participation:

- Undergraduate research involvement through the new Experimental Mathematics Lab
- 16 teams of undergraduates

CAREER CNS-1652238, University of Colorado Bouler, PI Katherine E. Stange