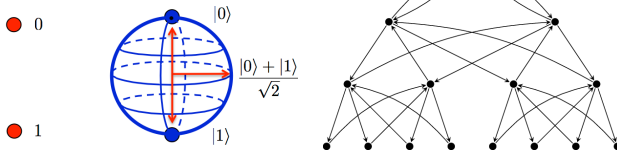


Quantum resistant elliptic curve cryptography

Thomas Gregersen



- ▶ I work on public key cryptography, an area which is going through a development phase to counter the threat of quantum computers if they ever become available.
- ▶ In theory, information may be stored on qubits which enable important computations to be performed at lower asymptotic complexity than what can be done classically.
- ▶ Today's algorithms (RSA/DH/ECDH typically) will be severely affected if such powers can be harnessed in full strength. This is not a given, but we must have quantum resistant alternatives at the ready if they do.

- ▶ In the process of finding new stand-ins for key agreement and signatures, the new algorithms are typically based on computationally hard problems found in coding theory, lattices and *isogeny-graphs* coming from elliptic curves¹.
- ▶ Isogeny-based cryptography is a young field which does not yet have a very long history of cryptanalysis or development to rest on, but is kept as a candidate for its promising traits.
- ▶ My project proposal is on this family: Start with the NIST-candidate SIKE² and CSIDH³ and describe their theoretical and practical foundations. Then, try to find ways in which they can be improved in terms of performance.

¹<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>

²<https://sike.org/>

³<https://csidh.isogeny.org/>

- ▶ There is also a possibility of looking into higher genus versions, but this assumes a strong mathematical background.
- ▶ To be able to work on this project, a good command of algebra is of the essence: You will need to know groups/rings/fields and will have to learn some algebraic geometry (elliptic curves) to succeed.
- ▶ The project may be more theoretical, but may also look into implementation issues by examining the above proposals along the way.
- ▶ If this project sounds interesting to you, send me an e-mail: thomas.gregersen@its.uio.no