NINA BINDEL, University of Waterloo and IQC
Post-quantum cryptography: faster, smaller, harder?

Large quantum computers will be able to break essentially all of our asymmetric cryptography used today, as Shor's quantum algorithm solves the discrete logarithm and prime factorization problem in polynomial time. To maintain security also in the future, researchers, industry and standardization bodies are busily constructing cryptographic algorithms whose security is based on problems that cannot be efficiently solved by known classical or quantum algorithms. Many of these "post-quantum" cryptographic algorithms are constructed over lattices with security based on the hardness of finding closest or shortest vectors in a lattice. For efficiency reasons, these hardness assumptions are tweaked, optimized, and tailored to the cryptographic algorithms and applications. In this talk we will give an overview into the topic of post-quantum cryptography and different variants of hardness assumptions in modern lattice-based cryptography. Furthermore, we will discuss known differences in the concrete hardness of these assumptions and open gaps.