Abstract for Research Exam

Mark Schultz

May 6, 2021

Lattice-based encryption has emerged as a leading candidate for both key-encapsulation mechanisms (KEMs) and digitial signature schemes that are secure against quantum-capable adversaries. These primitives are of vital importance in Transport Layer Security (TLS), which is a backbone of the modern internet. While a variety of lattice-based KEMs exist, they tend to fall into two frameworks, which we call *reconcilliation*[1]*-based KEMs* and *encryption-based KEMs*. Within each of these frameworks, one can modify:

1. The underlying hardness assumption under consideration (such as using Ring/Module learning with errors rather than "plain" LWE)
2. The algebraic object (ring/module) where arithmetic occurs
3. Certain coding-theoretic constructs that are implicit within schemes

to obtain a diversity of schemes, including NIST PQC finalists.

We analyze several formalizations of the above two frameworks, after modifying them to incorporate several common communication-saving optimations that occur in practice, but have been omitted from the frameworks. We then benchmark these frameworks against the NIST PQC finalists, and explore how modifying the implicit coding-theoretic constructs can impact the final rate of the constructions.

[1] These are also often called "Noisy Diffie-Hellman" constructions.