Papers and Abstracts for "Meta Lattice-based Encryption and KEMs"

Mark Schultz

April 22, 2021

1 Introduction

In my research exam, I plan to examine *lattice-based Key Encapsulation Mechanisms* (KEMs). A KEM allows two users to agree on a shared secret over an authenticated (public) channel. This is the basis of most secure communication on the internet, where generally schemes based on the Diffie-Hellman assumption are examined (originally over finite fields, but in recent years over elliptic curve groups as well). There has been significant software engineering effort to implement, optimize, and deploy such schemes, generally through a protocol known as the *Transport Layer Protocol* (TLS).

Unfortunately, it is well-known that all such schemes are insecure against attacks by quantum computers. Due to an abundance of caution, there is tremendous interest in developing replacements for such protocols now (while quantum computing is still in its infancy). Lattice-based cryptography[1] has emerged as a leading foundation for these new sets of protocols, both in academia, and in a recent NIST cryptographic standardization contest.

Abstractly, it is known that one cannot hope for a "drop-in" replacement for the former Diffie-Hellman-type schemes (by replacing the elliptic curve group with some "better group"). There are roughly two lines of work trying to get around this inconvience:

1. Relaxing Diffie-Hellman type schemes to work with "almost groups" (generally called group actions[2]), as done in the isogeny-based cryptography community

[1] Here when I say "lattice-based cryptography", I should more properly say "LWE/LWR-based cryptography". There is a separate lattice-based cryptographic assumption one can use to build cryptographic primitives (NTRU), and I have seen some attempts to compare it with LWE-based cryptography, but they are quite informal, and due to LWE's better security properties I focus on it.

[2] In short, in groups one can multiply any two elements, i.e. you have a product $G \times G \to G$. A group action on a set X gives a "product-like" operation $G \times X \to X$. Any group acts on $X = G$ via the standard product. One can view this as using a "partial" (as in not defined for all inputs) product rather than a total one.

2. Relaxing Diffie-Hellman type schemes to be "noisy" Diffie-Hellman type schemes, as done within the lattice-based cryptography community

In my research exam, I plan to survey the noise intrinsic to lattice-based KEMs, and the variety of coding-theory techniques one can use to correct it. The goal of this is to provide a uniform perspective on lattice-based KEMs, and isolate the coding-theoretic techniques implicitly used within them, with the hope of this allowing one to use more advanced coding-theoretic techniques. Moreover, if one fixes a "framework" for building KEMs, this constrains the design space of KEMs in a way that one can use to prove impossibility results on KEMs designed in such a framework.

To accomplish the above task, I plan on examining both lattice-based KEMs, and other frameworks that authors have suggested for this approach (I list two inequivalent ones among the list of papers below). Throughout, my goal will be to compare the abstract techniques used, as the particular efficiency of schemes requires a uniform way to discuss schemes of the "same security level", which is not a fully solved question within lattice-based cryptography.

2 Papers and Abstracts

I order the papers in the following way:

1. The first few papers present frameworks for lattice-based KEMs, although the second paper additionally proves rate bounds within this framework

2. After this, the papers will be papers on concrete lattice-based schemes, prioritizing historically important ones, as well as papers detailing leading NIST competition candidates (say schemes that reached at least round 2 out of 3)

2.1 Frameworks

As mentioned before, there are a few papers that have formalized frameworks for LWE-based key exchange. Most of these frameworks are implicit within the literature, so the novel contribution of the paper is either making this framework explicit, or doing something interesting with the framework.

Throughout this, define the function $\mathsf{LWE}(s)$ as a function which samples a, e randomly from appropriate distributions[3], and outputs:

$$\mathsf{LWE}(s, a, e) = (a, as + e) \tag{1}$$

a, s, e live in a ring[4], i.e. an object where addition, multiplication, and subtraction are defined (but not always division). I will often refer to $\mathsf{LWE}(s, a, e)[0] = a$

[3]The distributions are quite standard, but are unimportant when describing things at this level. One should know that a is roughly uniformly random, and e is "small", i.e. potentially correctable with an error-correcting code (a is not).

[4]This is not strictly true, but it is better to think this informally at this point.

as a, and $\mathsf{LWE}(s, a, e)[1] = as + e$ as b, as is standard in the community. The terms a, s, e as live in a ring[5], i.e. an object where addition, subtraction, and multiplication are well-defined.

I will first sketch frameworks for lattice-based encryption, and lattice-based KEMs, before writing abstracts for all of the relevant papers. It may be the case that for any particular paper that the framework under consideration differs slightly from the framework presented below, but these differences are small enough that summarizing the papers in terms of the below frameworks will allow for a succint summary of the relevant papers with little loss in conceptual clarity.

2.1.1 Lattice-Based Encryption

The hardness assumption within lattice cryptography is that $(a, as+e) \approx_c (a, u)$ is pseudo-random, so one can then use u as a one-time pad to encrypt a message, by setting $b = b + m$. Decryption computes $b - as = m + e$, so decryption may be incorrect. One can fix this by encoding m with an "error-correcting code", which can remove the error e from $m + e$.

2.1.2 Lattice-Based KEMs

If Alice and Bob sample $\mathsf{LWE}(s_i, a_i, e_i)$ for $i \in [2]$, and each sends their b_i value to the other, then they can compute:

$$(a_0 s_0 + e_0)a_1, \qquad (a_1 s_1 + e_1)^t \tag{2}$$

one only needs the transpose when working with MLWE/LWE (and not RLWE), i.e. when the ring is a matrix ring, but this is a small detail[6].

These both have "main term"

2.1.3 Limits on the Efficiency of (Ring) LWE based Non-interactive Key Exchange

This work formalizes a framework for lattice-based KEMs based on a technique known as *error-reconciliation*. It parameterizes this framework in terms of an underlying choice of "reconcilliation function", and studies the possibility of *non-interactive* reconcilliation functions. In this framework, they prove impossibility of many natural kinds of reconcilliation, and show that any non-interactive reconcilliation instantiation must use a reconcilliation function which *itself* has cryptographic properties (namely, it is a kind of pseudorandom function). Most reconcilliation functions which have been considered have purely coding-theoretic properties, i.e. they are "covering codes".

[5] Again this is not technically true, but explaining this at this stage will only complicate things for little gain.

[6] Essentially, when working over non-commutative rings one has to be more careful about the precise expressions used to ensure correctness, but this is a technical point, rather than a conceputal one.

2.1.4 Wyner Ziv Reconcilliation for Key Exchange based on Ring-LWE

This paper formalizes a KEM framework where reconcilliation is done via a technique known as (lattice-based) *vector quantization*, i.e. solving CVP with respect to some overlattice of the lattice "used for error-correction". There are some slight issues with this simplistic framing (namely that the KEM "encrypts the zero message", which is typical, so no lattice is *literally* used for error correction.), but the main idea of the paper is to connect an informal technique in lattice cryptography with a formally studied technique (Wyner Ziv coding) in coding theory.

This paper is quite interesting, but while an explicit framework that admits non-trivial quantizers[7] is *proposed*, all instantiations of the framework only use trivial quantization, and the general analysis done is where the quantizer is "hard-wired" to be trivial, which is somewhat disappointing.

2.1.5 A Framework for Cryptographic Problems from Linear Algebra

This paper notices that:

1. LWE-based cryptography
2. Coding-based cryptography
3. "Mersenne Prime"-based cryptography (which one can view as a "big integer" version of LWE-based cryptography in a certain way).

can all be phrased in terms of a (family of) abstract cryptographic schemes based on arithmetic in free modules over quotients of polynomial rings, where one varies:

- The choice of underlying ring
- The "size" of "small" elements

I find this particular work fascinating — the connection between LWE-based and Coding-based (more properly LPN-based) cryptography is standard, but I was unaware of the connection to "Mersenne Prime"-based cryptography. Moreover, the parameterization of schemes into some "choice of arithmetic system" and "a notion of small elements" was intuitively how I intuitively thought about things like this already.

2.2 Error Correcting Codes

The rest of the papers will survey design choices used in practice in the design of lattice-based encryption/KEMs. I wish to explore the different coding-theoretic

[7] "Non-trivial" here means that the quantizer, as a covering code/lossy compression scheme, is not simply the identity.

choices made, so will look at the different underlying codes used. The papers surveyed will try to be a representative sample by covering:

- Techniques that are widespread within the field (by my own subjective opinion)
- Techniques that are compelling to make it into NIST round 2 (or better) candidates

I will also include certain papers that do not fit into the above categories but are still interesting, but will cover the above two at a minimum.

The papers examined will try to highlight the diversity of codes (implicitly) used, focusing on:

- Techniques that are widespread within the field
- Techniques that are compelling enough to be used in NIST-PQC round 2 or better candidates

While this

2.2.1 Regev Code

2.2.2 Dual Regev Encryption

2.2.3 Power of Two Code

2.2.4 Dual Power of Two Code

2.2.5 Leech Lattice

2.2.6 LWR

2.3 Quantizers

2.3.1 NewHope / D4

2.3.2 NewHopeSimple

2.3.3 Repetition Code