Papers List for Research Exam

Mark Schultz

March 29, 2021

1 Introduction

I intended to do my research exam on certain coding-theoretic design choices implicit within lattice-based cryptography (specificlly, encryption and Key Encapsulation Mechanisms). This roughly can be studied from two directions:

1. **Formal**: By proposing "frameworks" that are parametrized by underling coding-theoretic choices, and then formally studing *these very frameworks*, i.e. studing the "best" possible implementations of the framework abstractly (by proving "lower bounds", or impossibility results).
2. **Practical**: By proposing explicit lattice-based encryption schemes/KEMs, which often *implicitly* are parameterized by the aforementioned coding-theoretic choices (i.e. by providing *constructions* of encryption schemes/KEMs).

I will therefore divide the papers in my annotated bibliography into these two categories. The "Practical" category *itself* will be further sub-divided, but I will discuss that when I get to it.

2 The Formal study of Encryption/KEMs

While there has been a general intuitive notion of what a framework for a lattice-based encryption/KEM should look like for some number of years, the following papers make this much more explicit than it is generally presented.

While (I believe) not directly relevant for the main purpose of the research exam, I myself have some results that would fit within this section (these are not yet published, but are ready to start being submitted places).

2.1 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 (vaguely, they are lossy compression schemes of a certain form).

2.2 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[1] 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. Finishing the analysis of this framework (and especially looking for non-trivial instantiations of it) would have been quite interesting.

2.3 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

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

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[2] 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.

3 The Practical Study of Encryption/KEMs

While there are a number of papers that I could include/are interesting for somewhat esoteric reasons, one of the best places to try to find "practical" encryption schemes/KEMs is in the NIST Post-Quantum Cryptography standardization contest. To this end, I will include all round 2 or better lattice-based[3] encryption schemes/KEMs. Note that this will include both LWE-based encryption schemes, and NTRU-based encryption schemes, which are subtly different in a way the "Framework for Cryptographic Problems from Linear Problems" paper makes quite clear. I will also include a number of non-NIST papers which I find personally interesting. For the NIST submissions, I will additionally include thier current status in the competition (which is in round 3, generally the final round, although there have been discussions of a round 4 for this particular competition).

To aid the cutting of potential papers, I will summarize the following things for the NIST submissions:

1. Place in the competition
2. Choice of "arithmetic" (ring computations take over, free module rank)
3. Choice of hardness assumption ("NTRU-like" or "LWE-like")
4. Underlying coding-theoretic choices

My main interest is in investigating the fourth point, especially as one can generally prove *much* stronger bounds against "coding-theoretic" properties than one can prove against "computational" properties. I already have some results of the above form (against the value of a "coding theoretic property" under any possible "coding-theoretic choice" of a certain framework), and my hope with this research exam is to:

1. Clarify the variety of frameworks that "practical" schemes fit into

[2] Or more properly of the entire *area* of Mersenne prime-based, cryptography.

[3] As the framework I like the most of the above is the "Cryptographic Problems from Linear Algebra" paper (which one can fit many *coding-based* constructions into as well), it might make sense to also survey LPN-based encryption schemes. There are other coding-based encryption schemes (rank metric ones) which it is unclear to me if they fit into the aforementioend framework, and due to my unfamiliarity with coding-based encryption I will limit my scope and not consider them.

2. Clarify the coding-theoretic choices *within* these frameworks which have been explored.

So essentially, my goal is to further study lattice-based encryption schemes/KEMs *formally*, but informed from *practice*.

3.1 NIST Round 2 Candidates

3.1.1 NewHope (and Simple)

RLWE based KEM (cyclotomic power two) for $n = 512, 1024$.

3.2 NIST Round 3 Candidates

3.2.1 KRYSTALS-KYBER (Finalist)

M-LWE based encryption scheme over the ring $\mathbb{Z}_q[x]/(x^{256}+1)$. Error-correction and quantization are done via the cubic lattice. The LWE error is binary. The matrix A is generated from the output of a PRF.

3.2.2 FRODOKEM (Alternate)

LWE-based KEM without reconcilliation (so uses the "encryption" framework). Uses inversion sampling w/ rounded continuous gaussian?

3.3 Misc. Other Interesting Constructions