Lattice Codes in Lattice Cryptography
Research Exam Annotated Bibliography

Mark Schultz

May 9, 2021

1 Introduction

In this research exam I am interested in investigating coding-theoretic techniques within lattice cryptography. These broadly fall into two categories:

1. Information-theoretic techniques to prove bounds in lattice cryptography
2. The use of error-correction techniques within lattice cryptography

I call the first part "frameworks", and the second part "codes". As there are fewer frameworks than instantiations, if a paper does both I will list it in the "frameworks" section.

2 Frameworks

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 [GKRS20]

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 [SLCPL]

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. Note that this paper does propose a non-trivial *error-correction* implementation using the Barnes-Wall Lattices.

2.3 A Framework for Cryptographic Problems from Linear Algebra[BCSV20]

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[2] to "Mersenne Prime"-based cryptography.

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

[2] Or more properly of the entire *area* of 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.

That being said, this does not directly connect to the rest of the research exam in that natural of a way. If one restricts back to thinking about purely lattices, I do not think this really says anything new.

3 Codes

3.1 The impact of error dependencies onRing/Mod-LWE/LWR based schemes [DVV19]

Typically in an LWE/RLWE/MLWE-based encryption scheme, one is able to get ℓ_p-bounds (generally for $p \in \{2, \infty\}$) on the error one must correct. A number of authors have investigated correcting this error using *binary* error-correcting codes, i.e. codes that can correct noise of bounded *Hamming* weight $\|w\|_0$. This is difficult to prove things theoretically about, as there is in general not a relationship[3] between $\|w\|_0$ and $\|w\|_p$ for $p > 0$ (so the notions of "small" are incompatible). As a result, authors have adopted the use of heuristic methods to analyze decryption failures. These heuristics have failed once already (as demonstrated in [DVV19], which I will likely include in my research exam as well), so I exclude binary error-correcting codes from my research exam/survey due to a lack of confidence with the current analysis of techniques in the subarea. I will likely include at least one paper of this form to highlight the issue with the analysis[4], but have not settled on one yet.

Instead I will focus on "lattice codes", which do not run into this issue/are defined with respect to the correct notion of "small". More generally if I end up parametrizing my survey in terms of an underlying arithmetic + notion of size, I will focus on error-correction which is defined with respect to that same notion of size.

3.2 Error Correction

There are a number of distinct lattice codes that are commonly used (implicitly) within the literature. In general, I briefly mention that given a k-dimensional lattice L, one can build a nk-dimensional lattice L for any $n \in \mathbb{N}$ by taking direct sums (this is similar to concatenating binary codes), so even in high-dimensional cryptographic setting fixed-dimension lattices are worthwhile.

[3] This should be contrasted with essentially every other ℓ_p norm. One can generally find bounds of the form $\|a\|_p \leq n^{f(p,q)}\|a\|_q$ relating an ℓ_p norm to an ℓ_q norm, where $f(q,p)$ is a generally simple function, when $p, q \geq 1$.

[4] Likely one before the heuristic was falsified so my inclusion is not of the form "look at this paper which is not familiar with the literature"

3.2.1 On Lattices, Learning with Errors, Random Linear Codes, and Cryptography [Reg]

While this paper does *much* more than just introduce the cubic lattice for error-correction (this part is really an afterthought), as error-correction using the cubic lattice is often called "Regev-type encryption" it seems sensible to cite this paper. In particular this uses the lattice $(q/2)\mathbb{Z}^n$ (a scaled cubic lattice) for error-correction.

3.2.2 Power of Two

This lattice really has two natural citations — to the paper that first uses it, and a paper that identifies a rather special property of it that has led to its widespread use in advanced applications. As I am not particularly concerned with these advanced applications, I will solely cite the first paper.

Lossy Trapdoor Functions and Their Applications [PW]: This is the first paper to introduce the "powers of two" lattice, and uses it to build what is known as a "lossy trapdoor function". The key property of it that it uses is (essentially) that it is simple to solve the "Short Integer Solution" problem on this lattice. There are some papers that generalize this property to other lattices, but I do not believe that is vital when considering the error-correction capabilities of this lattice.

3.2.3 Chinese Remainder Theorem

While the chinese remainder theorem has appeared earlier within lattice cryptography (to simplify arithmetic in $\mathbb{Z}/q\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i\mathbb{Z}$, or to additionally simplify arithmetic in $\mathbb{Z}[\zeta_n] \cong \prod_i \mathbb{Z}[x]/(x - \zeta_n^i)$), I am particularly interested in its use for error correction. This (among some other things) is covered in **Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More** [GMP19]. This paper can be thought of as a "special case" of what I want to survey — it looks for encoding of messages that both correct error, and have a certain "small preimage" property. I am interested in investigating solely the error-correction capabilities of encodings.

3.2.4 Dual Power of Two

In **Compressible FHE with Applications to PIR** [GH19], a certain encoding is described which uses a "nearly square gadget" matrix. While not described this way, this encoding can equivalently be described as encoding onto the dual lattice of the aforementioend "power of two" encoding. This particular construction "trades off" rate and error-correction capability.

Note that the other error-correction techniques mentioned are all (up to scaling) self-dual, so do not have corresponding "dual" constructions.

3.2.5 Leech Lattice

In **Cryptographic Decoding of the Leech Lattice** [vP], error-correction with the Leech Lattice Λ_{24} is investigated. This is a highly symmetric lattice with many remarkable properties, including being a quite efficient (and provably the best) packing of 24-dimensional space. The only other dimensions that such packings are explicitly known in are 1, 2, 3, 8, and 24.

The paper gets some rate improvements over more naive encoding methods, but the leech lattice being 24 dimensions does not work well with standard cryptographic conventions. A common usecase for public key encryption is to encrypt a 256 bit AES key (this is called "hybrid encryption"). If one uses (direct sums of) the Leech lattice for this, one is left with a lattice of dimension $\in \{240, 264\}$, so one must "waste a little space" to do hybrid encryption, which negates some of the rate savings that the technique has.

As a result, an interesting thought is to redo the aforementioned analysis with the extremal lattice in 8 dimensions (as $8 \mid 256$), known as the *Gosset lattice*. I do not believe anyone has done this yet, and it should not take too long to do.

3.3 Quantization

There are a variety of constructions in the literature that encrypt a message using the aforementioned error-correction paradigm, and then "round" the resulting value to some "nearest point". The most basic form of rounding is to the nearest integer point, i.e. $\mathbb{Z}^n$, but as we will describe there are more clever things one can do.

3.3.1 LWR / rounded cubic

As mentioned, the most basic thing one can do is round to the nearest integer. This rounding technique often is paired with a slightly different hardness assumption (known as *Learning with Rounding*), where instead of assuming that:

$$(A, As + e) \approx_c (A, u)$$

is pseudorandom, one assumes that:

$$(A, \lfloor As \rceil) \approx_c (A, u)$$

is pseudorandom. This technique can yield some rate savings, as one can effectively "throw away" noisey low-order bits.

If one is ok with introducing other randomness, i.e. computing $(A, \lfloor As + e \rceil)$, then on could base hardness on the LWE assumption while appealing to rounding to other lattices. This is (roughly) what is done in the other papers I consider.

3.3.2 Repetition

A particularly interesting quantizer is used in **Leveraging Linera Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles** [BDGM19]. This work (implicitly) rounds points to the lattice $(1, 1, \ldots, 1)+q\mathbb{Z}^n$, which is the "construction A" applied to the standard repetition code. This construction yields asymptotically rate 1 encryption from polynomial modulus, which is novel (prior constructions required super-polynomial modulus), and a large motivation into looking into this topic in the first place.

3.3.3 D_4

(Direct sums of) the D_4 lattice were used to quantize in the design of the NewHope KEM [ADPS15]. This quantizer is paired with a method of encoding a single bit into "4 dimensions", which I believe can be modeled as an error-correcting code.

This KEM also has a varient where one rounds to the cubic lattice instead of direct sums of the D_4 lattice (this version was actually submitted to the NIST PQC competition) [AAB$^+$]. This yields a mild (roughly 5%) degredation of parameters while being much simpler to work with.

I have some reason to believe that one could use different quantization to great effect. Namely, that for a certain formalizataion of "intrinsically high dimensional lattices" (of which neither $\bigoplus \mathbb{Z}$ and $\bigoplus D_4$ are, as they are both direct sums of low dimensional lattices), I have some evidence that quantization has significant limits to its effectiveness.

4 Ideas I would like to explore

I have some concurrent work with Daniele Micciancio on this topic, and have proved various rate bounds on encryption/KEMs. The framework these bounds are proved in allows key material to be distribtued "for free", which is perhaps not the most useful framework for KEMs (and instead is useful for private-key encryption for FHE purposes — one can distribute some small seed, and use a PRG to expand it to the large amount of required key material).

This work has given me a few ideas of (potentially) concretely useful instantiations of lattice-based KEMs/error-correction which are absent from the literature. At least, I would like to explicitly consider:

1. An instantiation of lattice-based encryption with respect to the Gosset lattice E_8 rather than the Leech lattice Λ_{24}. The leech lattice scheme was quite performant, but suffered from the issue that $24 \nmid 256$, so is not well-adapted to the existing social conventions on hybrid encryption. As $8 \mid 256$, the Gosset lattice may still be useful in this setting.

2. An instantiation of the NewHope KEM with an "intrinsically high dimensional quantizer". My concurrent work with Prof. Micciancio makes me think this may be much more performant than either of the quantizers

NewHope has suggested (either the cubic lattice, or direct sums of the D_4 lattice). It could perhaps be interesting to examine other intrinsically high dimensional lattices for this purpose — for example D_{1024} itself. There is a certain formal sense that D_n and the repetition lattice are closely related (D_n is a "$q = 2$" version of the q-ary repetition lattice).

References

[AAB+] Erdem Alkim, Roberto Avanzi, Joppe Bos, Léo Ducas, Martin R Albrecht, Emmanuela Orsini, Valery Osheter, Kenneth G Paterson, Guy Peer, and Nigel P Smart. Algorithm Specifications and Supporting Documentation. page 47.

[ADPS15] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - a new hope. Technical Report 1092, 2015.

[BCSV20] Carl Bootland, Wouter Castryck, Alan Szepieniec, and Frederik Vercauteren. A framework for cryptographic problems from linear algebra. *Journal of Mathematical Cryptology*, 14(1):202–217, July 2020.

[BDGM19] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Leveraging Linear Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles. Technical Report 720, 2019.

[DVV19] Jan-Pieter D'Anvers, Frederik Vercauteren, and Ingrid Verbauwhede. The Impact of Error Dependencies on Ring/Mod-LWE/LWR Based Schemes. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, volume 11505, pages 103–115. Springer International Publishing, Cham, 2019. Series Title: Lecture Notes in Computer Science.

[GH19] Craig Gentry and Shai Halevi. Compressible FHE with Applications to PIR. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography*, volume 11892, pages 438–464. Springer International Publishing, Cham, 2019. Series Title: Lecture Notes in Computer Science.

[GKRS20] Siyao Guo, Pritish Kamath, Alon Rosen, and Katerina Sotiraki. Limits on the Efficiency of (Ring) LWE based Non-Interactive Key Exchange. Technical Report 1555, 2020.

[GMP19] Nicholas Genise, Daniele Micciancio, and Yuriy Polyakov. Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology EUROCRYPT 2019*, volume 11477, pages 655–684. Springer International Publishing, Cham, 2019. Series Title: Lecture Notes in Computer Science.

[PW] Chris Peikert and Brent Waters. Lossy Trapdoor Functions and Their Applications. page 41.

[Reg] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. page 37.

[SLCPL] Charbel Saliba, Laura Luzzi, Universite Cergy-Pontoise, and Cong Ling. Wyner-Ziv reconciliation for key exchange based on Ring-LWE. page 8.

[vP] Alex van Poppelen. Cryptographic decoding of the Leech lattice. page 63.