IMPERIAL

On the subject of lattices

and why cryptographers love them

Joshua Limbrey

2024-03-22

Agenda

01 What is currently used for cryptography?
02 What is a lattice?
03 What are these “hard lattice problems’?’
04 What can we do with them?
05 How we create post quantum schemes?
06 Some you may have heard of
07 Where next?
08 Further reading

What is currently used for cryptography?

- Diffie-Hellman
- El Gamal
- RSA
- DSA
- ECDSA
- ECDH
- Ed25519

All public key cryptography relies on what is called a **trap-door function**.

Easy to go one way *(encrypt)*, difficult to go the other *(decrypt)* without knowledge of a secret *(private key)*.

All of the schemes listed to the left are all dependant on the hardness of **prime factorisation** or the **discrete logarithm problem**.

Why are we bored of these?

These schemes have been around for a while (some nearly 50 years). The security against a standard adversary has been extensively studied, and the hardness of the problems fairly well understood.

Challenging to construct new and interesting forms of encryption (such as *homomorphic encryption*) due to the properties of the underlying problems.

Shor's algorithm[a] means that given an adversary with a sufficiently strong quantum computer, these schemes are no longer secure.

[a] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

(Above) Cryptographers wanting new toys, circa 2000 (colourised)

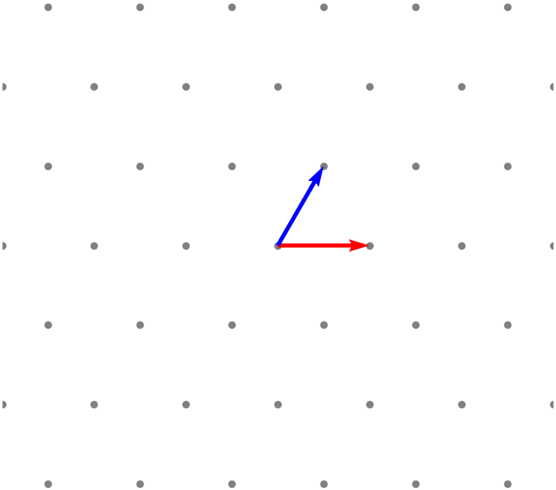
What is a lattice?

Definition: Lattice

The set of all linear integer combinations of basis vectors,

$$\mathcal{L} = \{\sum_{i=1}^{d} \mathbf{b}_i \mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^d\}$$

$$\mathbf{B} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}$$



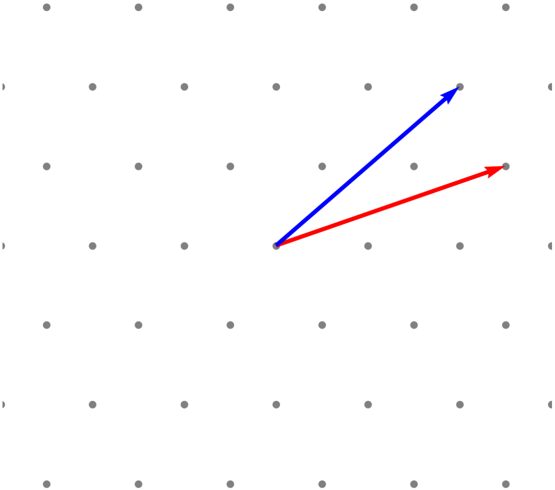
What is a lattice?

Definition: Lattice

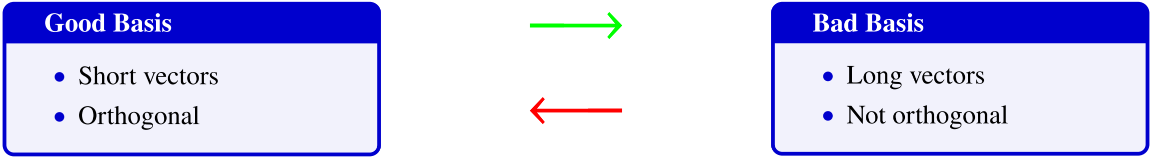
The set of all linear integer combinations of basis vectors,

$$\mathcal{L} = \{\sum_{i=1}^{d} \mathbf{b}_i \mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^d\}$$

$$\mathbf{B}' = \begin{pmatrix} \frac{5}{2} & 2 \\ \frac{\sqrt{3}}{2} & \sqrt{3} \end{pmatrix}$$



What is a lattice?



Good Basis

- Short vectors
- Orthogonal

Bad Basis

- Long vectors
- Not orthogonal

This process of going from a bad to good basis is called **basis reduction**.

LLL

- Polynomial runtime (in dimension)
- Exponential approximation (in dimension)

BKZ

- Exponential runtime (in blocksize)
- Exponential approximation (in blocksize)

HKZ

- Exponential runtime (in dimension)
- Optimal output

What are hard lattice problems?

Definition: Shortest Vector Problem (SVP)

Given a lattice, find the shortest *non-zero* lattice point.

Definition: Learning With Errors Problem (LWE)

Let, $\begin{bmatrix} \mathbf{b} \end{bmatrix} = \begin{bmatrix} \quad \mathbf{A} \quad \end{bmatrix} \begin{bmatrix} \mathbf{s} \end{bmatrix} + \begin{bmatrix} \mathbf{e} \end{bmatrix}$. Knowing *only* the values in green, find $\begin{bmatrix} \mathbf{s} \end{bmatrix}$.

Definition: Lattice Isomorphism Problem (LIP)

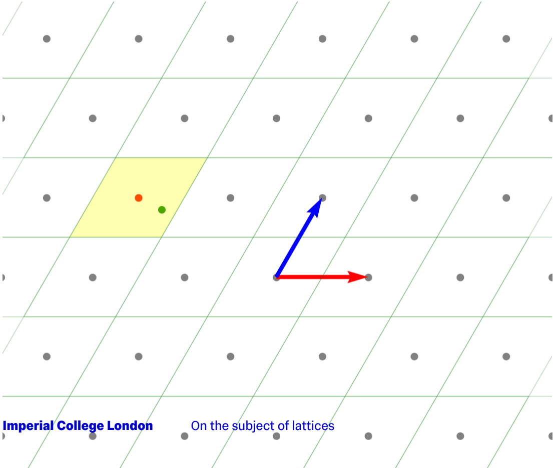
Given two lattices, $\mathcal{L}_1$ and $\mathcal{L}_2$, find the scaling factor and rotation to send one to the other (if it exists).

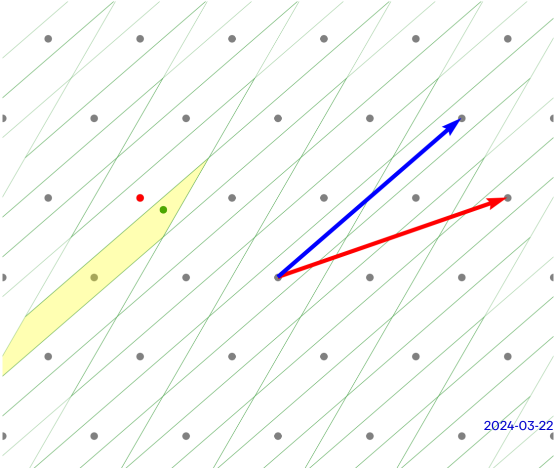
But we also have the Short Integer Solutions problem (SIS), the NTRU problem, the Closest Vector Problem (CVP), and all the many variants of anything mentioned here!

Closest Vector Problem

Definition: Closest Vector Problem (CVP)

Given a lattice and a random point, find the closest lattice point.





Learning With Errors

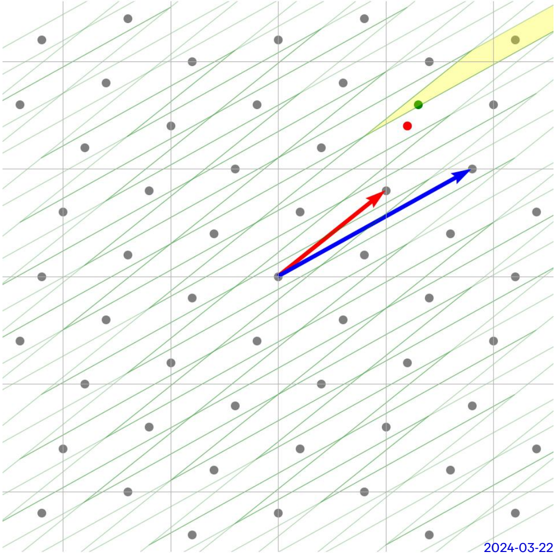
Learning With Errors Problem (LWE)

$$\begin{bmatrix} \mathbf{b} \end{bmatrix} = \begin{bmatrix} & \mathbf{A} & \end{bmatrix} \begin{bmatrix} \mathbf{s} \end{bmatrix} + \begin{bmatrix} \mathbf{e} \end{bmatrix}$$

We can construct what is called a q-ary lattice using $\mathbf{A}$.

Then, taking the target vector $\mathbf{b}$, solving a CVP instance *should* give us $\mathbf{As}$, and therefore $\mathbf{s}$.

Unfortunately, if the LWE parameters are chosen well, we do not get a good basis for our new lattice, and so solving CVP is hard.



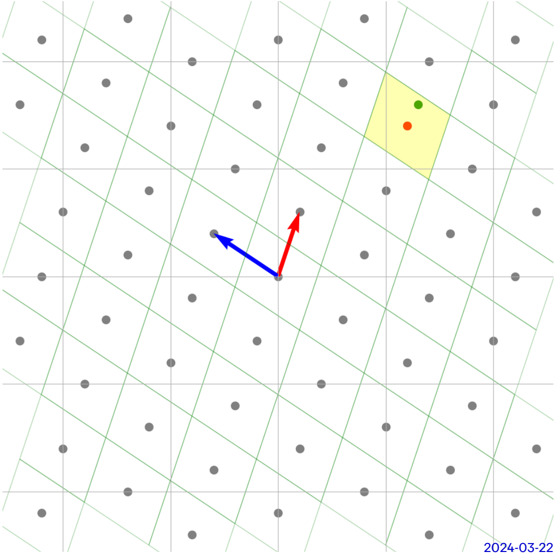
Learning With Errors

Learning With Errors Problem (LWE)

$$\begin{bmatrix} \mathbf{b} \end{bmatrix} = \begin{bmatrix} \quad \mathbf{A} \quad \end{bmatrix} \begin{bmatrix} \mathbf{s} \end{bmatrix} + \begin{bmatrix} \mathbf{e} \end{bmatrix}$$

With a good basis for our lattice, something that can be kept secret, solving CVP and recovering the secret is easy, however.

In practice, we have methods of turning a bad basis into a good basis (*lattice reduction*), but these algorithms do not scale well for high dimension lattices.



Lattice Isomorphism Problem

Lattice Isomorphism Problem (LIP)

Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, find the *isometry* between the two lattices.

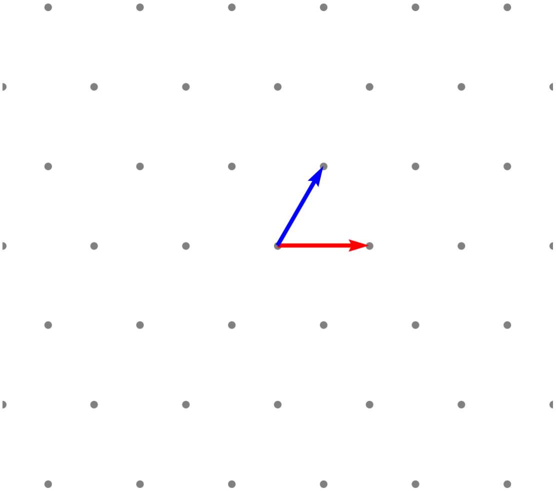
In other words, find the translation that describes the rotation that sends $\mathcal{L}_1$ to $\mathcal{L}_2$.

This is the A_2 lattice, the densest sphere packing in two dimensions.

Here, the rotation is 90°, with a scaling factor of 1.

Lattice Isomorphism Problem

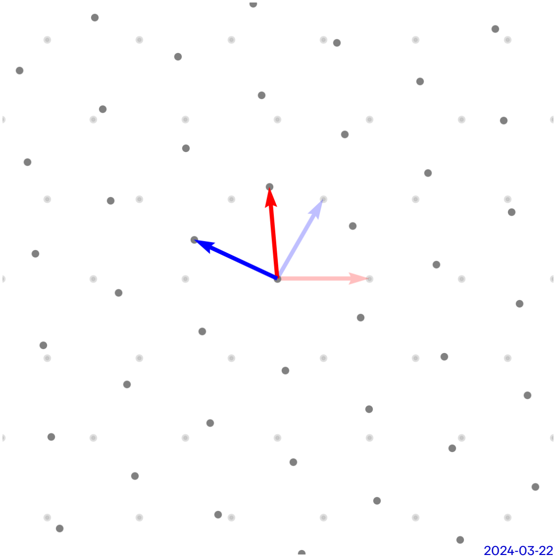
First, we take a lattice that has nice properties (dense, good decoding etc.).



Lattice Isomorphism Problem

First, we take a lattice that has nice properties (dense, good decoding etc.).

Then, we apply some **unimodular** transform. This equates to a rotation of our original lattice, and we say that these two are **isomorphic**.

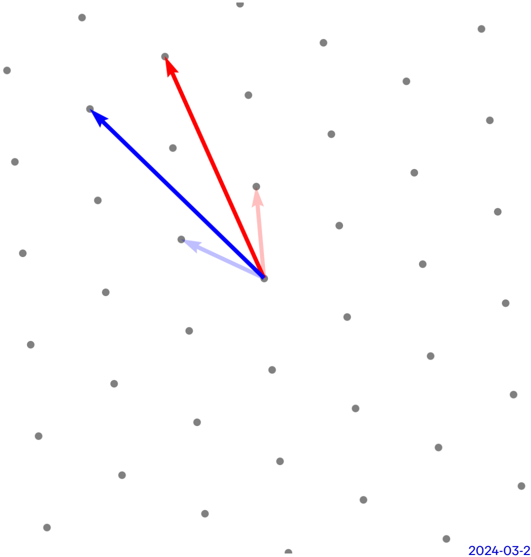


Lattice Isomorphism Problem

First, we take a lattice that has nice properties (dense, good decoding etc.).

Then, we apply some **unimodular** transform. This equates to a rotation of our original lattice, and we say that these two are **isomorphic**.

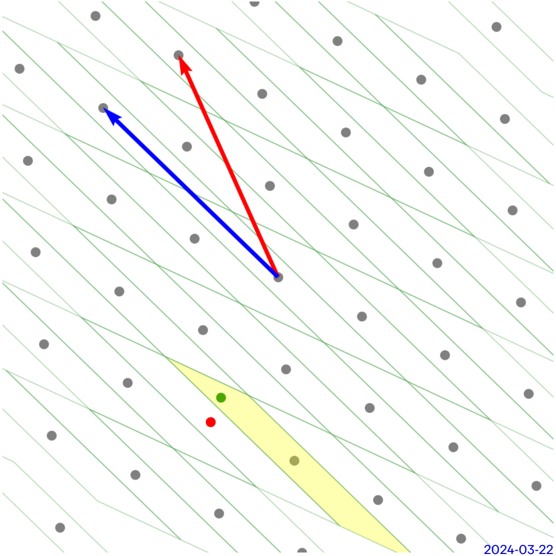
Finally, we hide this rotation with a basis transform; we make a bad basis of this isomorphism.



Lattice Isomorphism Problem

To encrypt, we take our message, a lattice point in the public lattice and add some small error.

Recovering this original lattice point using the (bad) public basis is hard to do.

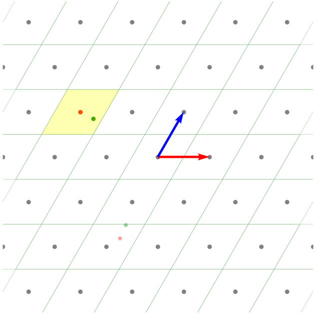


Lattice Isomorphism Problem

To encrypt, we take our message, a lattice point in the public lattice and add some small error.

Recovering this original lattice point using the (bad) public basis is hard to do.

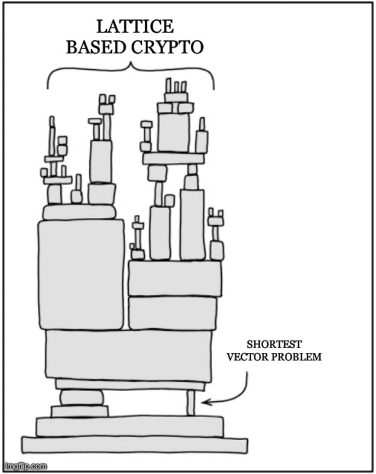
Knowing the rotation, we can convert this back to our original lattice, which we know a good basis for, and can easily recover the corresponding lattice point.



It's all SVP?

(Above) Regev discovering the the LWE to γ-SVP reduction, 2005

But don’t worry, even though all of these problems are reducible to SVP, they all work in slightly different ways, giving the schemes we build from them different properties (speed, key size, etc.).



(Above) xkcd Dependency, lattice based cryptography special edition

The PQC timeline

- **Deprecated**:
  the algorithm and key length/strength may be used, but there is some security risk. Assess risk before using a deprecated algorithm or key length.

- **Disallowed**:
  the algorithm, key length/strength, parameter set, or scheme is no longer allowed for the stated purpose.

Scheme	**Deprecated** *(112 bit strength only)*	**Disallowed**
Key Establishment		
Finite Field DH and MQV	2030	2035
Elliptic Curve DH and MQV	2030	2035
RSA	2030	2035
Signatures		
ECDSA	2030	2035
EdDSA	-	2035
RSA	2030	2035

Replace with:

Key Establishment

- ML-KEM

Signatures

- ML-DSA
- SLH-DSA
- LMS, HSS
- XMSS

What does all this mean for me?

- You should begin to use hybrid encryption now
  - Especially if a “harvest now, decrypt later” threat is relevant to you
  - Have the fallback of ECC if PQC is broken
  - Schemes such as X-wing and Xyber768
- For most people, this is as simple as upgrading your browser and dependencies (most crypto is dependent on upstream libs like openSSL)

> *“Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC). To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035.”*[1]

[1] J Biden. *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. National Security Memorandum 10. 2022. URL: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

Further reading

General Cryptography:

Lattices and Lattice Cryptography:

PQC Implementations:

Policy, Migration, and Standardisation:

IMPERIAL

Thank you