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.

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

[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.

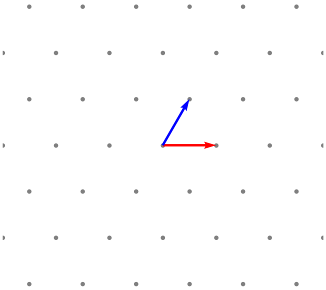
What is a lattice?

Definition: Lattice

The set of all linear integer combinations of basis vectors,

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

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



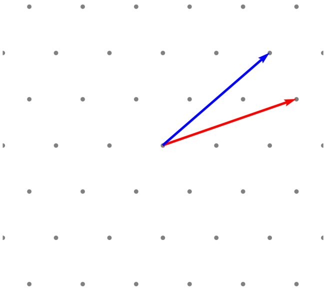
What is a lattice?

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 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!

Learning With Errors

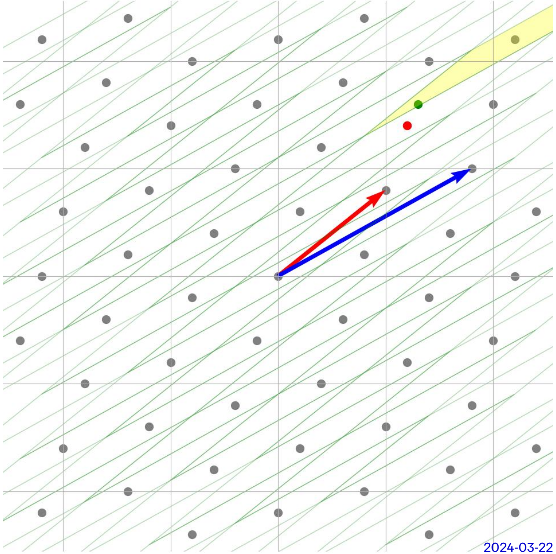
Learning With Errors Problem (LWE)

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

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 $\mathbf{A}\mathbf{s}$, 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.



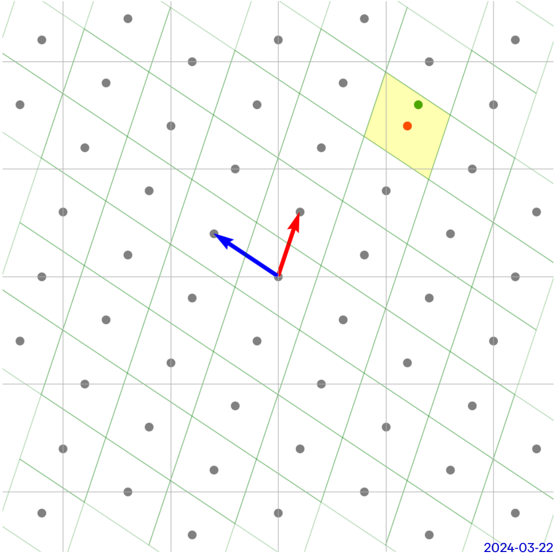
Learning With Errors

Learning With Errors Problem (LWE)

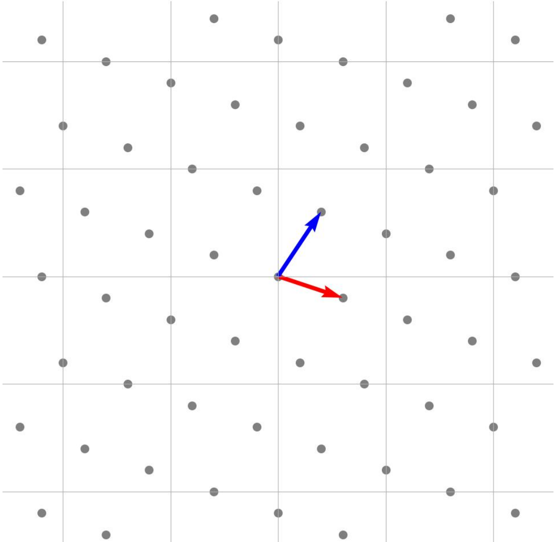
$$\begin{bmatrix} \\ \mathbf{b} \\ \\ \end{bmatrix} = \begin{bmatrix} & & \\ & \mathbf{A} & \\ & & \end{bmatrix} \begin{bmatrix} \\ \mathbf{s} \\ \\ \end{bmatrix} + \begin{bmatrix} \\ \mathbf{e} \\ \\ \end{bmatrix}$$

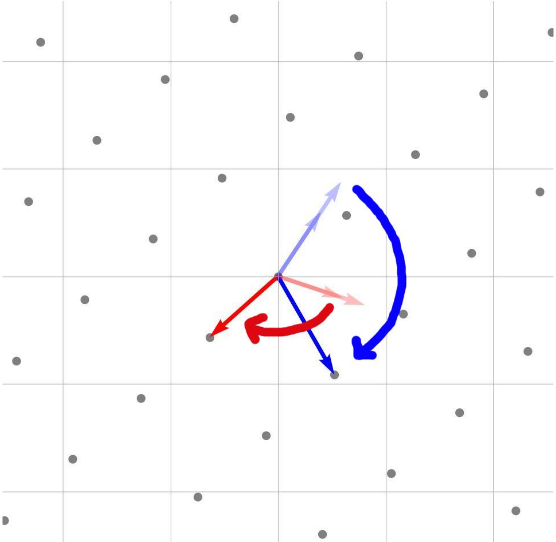
With a good basis for our lattice, something that can be kept secret, solving CVP and recovering the secret is easy, however.

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 (in the wild)

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 and scaling factor that sends $\mathcal{L}_1$ to $\mathcal{L}_2$.

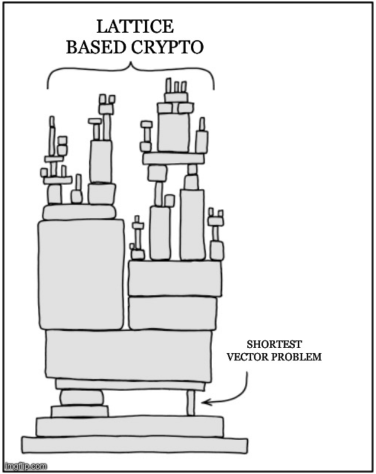
This is the A_2 lattice, the densest sphere packing in two dimensions.

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

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

What can we do with lattices?

Fully Homomorphic Encryption

FHE allows computations to be applied on encrypted data without needing to be decrypted first. This allows a user to allow a semi-trusted third party to operate on their data, without being able to access it, in such a way that when the user decrypts their data the same operations have been applied to the plaintext.

Secure Multiparty Computation

Similar to FHE, MPC is a privacy preserving construct in which a number of participants all want to compute a value as a public function of each of their private data. MPC allows them to do so whilst maintaining the secrecy of their inputs.

Cryptanalysis of Classical Schemes

Lattices are also used by cryptographers when attacking classical schemes such as RSA and ECC. They typically exploit weaknesses in parameter generation and utilise the collection of many signed messages by a single key[a].

[a] N. Howgrave-Graham and N.P. Smart. *Lattice Attacks on Digital Signature Schemes*. Designs, Codes and Cryptography, 23, 283-290. 2001. URL: https://link.springer.com/article/10.1023/A:1011214926272.

Post-Quantum Cryptography

It is believed that these lattice problems are hard to solve even on quantum computers.

Some schemes you may have heard of

LWE Based

ML-KEM/Kyber and ML-DSA/Dilithium

ML-KEM[a]/DSA[b] were both elected by NIST as schemes for standardisation, with the standards published August 2024. These are both front runners due to their speed, however their drawback is a fairly large key size. LWE is a well studied assumption, with strong worst and average case analysis.

[a] R. Avanzi et al. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. NIST FIPS 203. 2024. URL: `https://csrc.nist.gov/pubs/fips/203/final`.

[b] R. Avanzi et al. *Module-Lattice-Based Digital Signature Standard*. NIST FIPS 204. 2024. URL: `https://csrc.nist.gov/pubs/fips/204/final`.

Where Can I Find This?

- Cloudflare now support x25519xML-KEM in CIRCL[a]
- Chrome supports x25519xML-KEM as default for TLS[b]
- liboqs, the open-quantum-safe x Microsoft fork of openTLS supports ML-KEM and ML-DSA[c]
- As of release 9.9, OpenSSH supports mlkem768x25519-sha256 by default[d]
- Amazon supports ML-KEM in hybrid in AWS Key Management Service[e]

[a] https://blog.cloudflare.com/post-quantum-to-origins/

[b] https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

[c] https://github.com/open-quantum-safe/liboqs

[d] https://www.openssh.com/releasenotes.html

[e] https://aws.amazon.com/kms/

Some schemes you may have heard of

NTRU Based

Falcon and NTRUPrime

Falcon[a] was selected as a digital signature scheme by NIST, however is yet to be standardised. NTRUPrime[b] was not selected for standarisation by NIST, but is another popular key encapsulation scheme.

[a] P.A. Fouque et al. “Falcon: Fast-Fourier Lattice-base Compact Signatures over NTRU”. In: 2020. URL: https://falcon-sign.info/falcon.pdf.

[b] D.J. Bernstein et al. *NTRU Prime*. Accessed 1 January 2025. URL: https://ntruprime.cr.yp.to.

Where Can I Find This?

- liboqs, the open-quantum-safe x Microsoft fork of openTLS supports Falcon and NTRUPrime[a]
- As of release 9.9, OpenSSH supports sntrup761x25519-sha512 by default[b]

[a] https://github.com/open-quantum-safe/liboqs

[b] https://www.openssh.com/releasenotes.html

Some schemes you may have heard of

LIP Based

HAWK

Hawk[a] is the youngest of all schemes listed, and is currently the only lattice based scheme left in NISTs call for additional signature schemes[b]. HAWKs biggest selling points are smaller keys and signatures compared to other (LWE) signature schemes whilst maintaining the speed of lattices.

Where Can I Find This?

- No where I could find yet...

[a] L. Ducas et al. *HAWK: Module LIP makes Lattice Signatures Fast, Compact and Simple*. Cryptology ePrint Archive, Paper 2022/1155. 2022. URL: https://eprint.iacr.org/2022/1155.

[b] National Institute of Standards and Technology. *Post-Quantum Cryptography Digital Signature Round 1 Additional Signatures*. Accessed: 2024-12-20. 2024. URL: https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures.

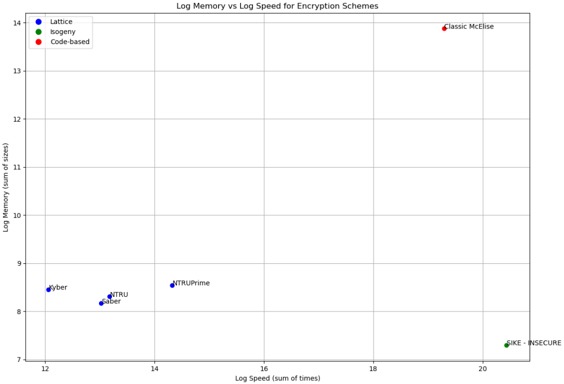
What if I don't want to use lattices?

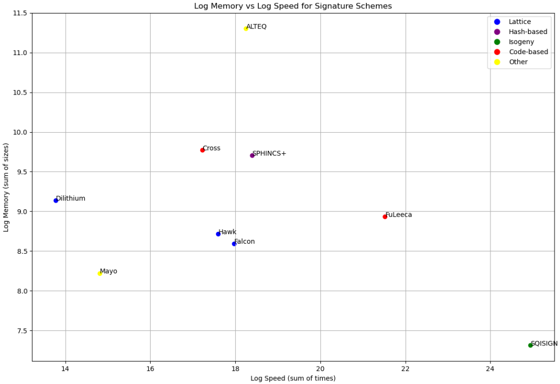
There are plenty of other foundations for PQC such as isogenies, cubic forms, and codes. In some cases, these might solve some issues we have with lattices *(key and signature size)*, but often with the trade-off of lattice benefits *(speed)*.

They can also let us create cool new applications, in the same way that lattices allow us to create fully homomorphic encryption, such as non-interactive key exchanges and verifiable delay functions.

Their biggest selling point is that they’re based on different hard problems - if SVP is broken in the same way that factoring was, we have something else to fall back on.

What if I don't want to use lattices?





Note: These are ***logarithmic*** *in scale. These are to give an illustrative and intuitive idea for performance of different schemes. In some cases, the experiments were run on different CPUs, and these values are the normalised logarithmic sum of all metrics. DO NOT USE THIS FOR SERIOUS EVALUATION.*

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