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 schemes are currently used for public key cryptography (signatures, key exchanges, etc.) today?

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)

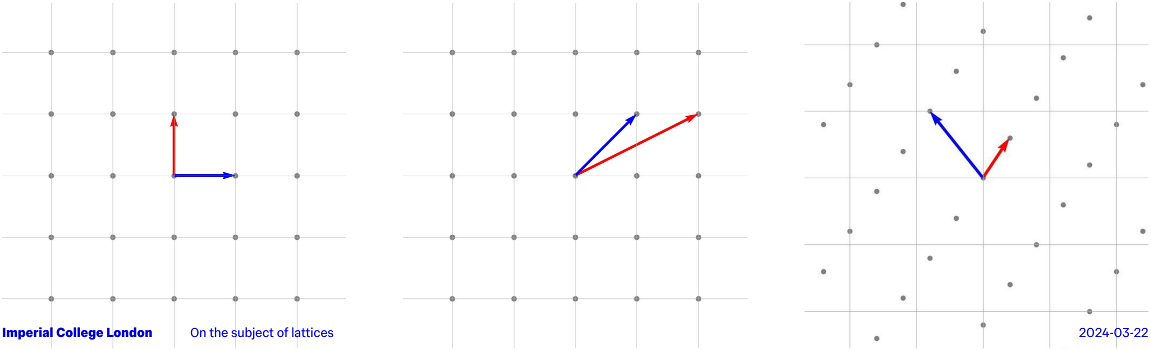
[a] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

What is a lattice?

Definition: Lattice

The set of all linear integer combinations of basis vectors,

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



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)

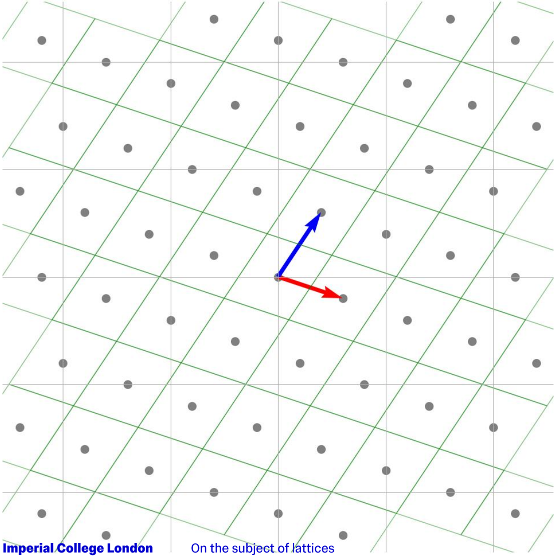
Let, $\begin{bmatrix} \\ \mathbf{b} \\ \\ \end{bmatrix} = \begin{bmatrix} & & \\ & \mathbf{A} & \\ & & \end{bmatrix} \begin{bmatrix} \\ \mathbf{s} \\ \\ \end{bmatrix} + \begin{bmatrix} \\ \mathbf{e} \\ \\ \end{bmatrix}$. Knowing *only* the values in green, find $\begin{bmatrix} \\ \mathbf{s} \\ \\ \end{bmatrix}$.

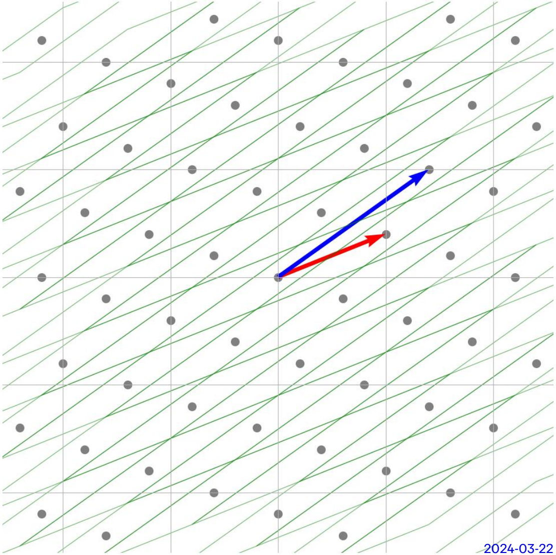
Definition: Lattice Isomorphism Problem (LIP)

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!

Shortest/Closest Vector Problem





Learning With Errors

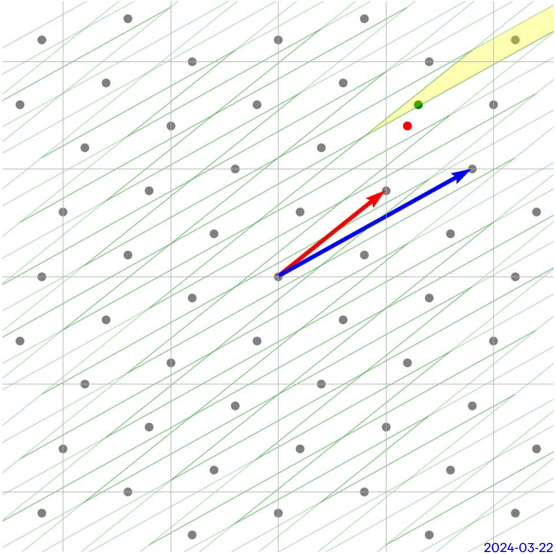
Learning With Errors Problem (LWE)

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

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.



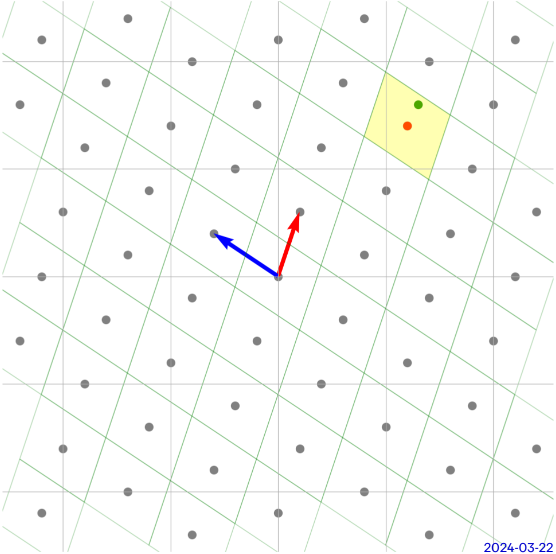
Learning With Errors

Learning With Errors Problem (LWE)

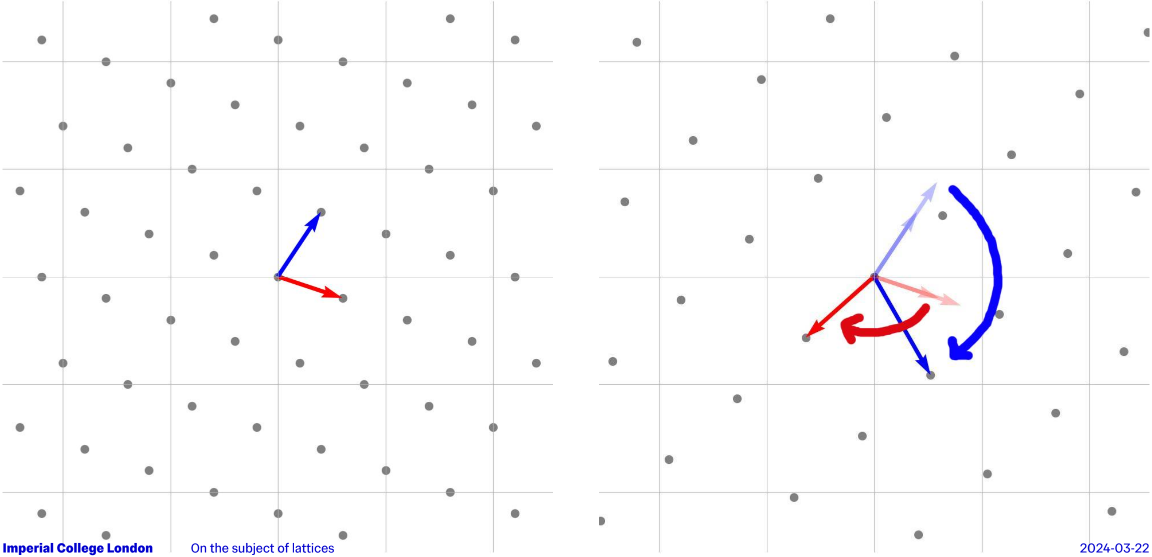
$$\begin{bmatrix} \mathbf{b} \end{bmatrix} = \begin{bmatrix} \quad \mathbf{A} \quad \end{bmatrix} \begin{bmatrix} \mathbf{s} \end{bmatrix} + \begin{bmatrix} \mathbf{e} \end{bmatrix}$$

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.



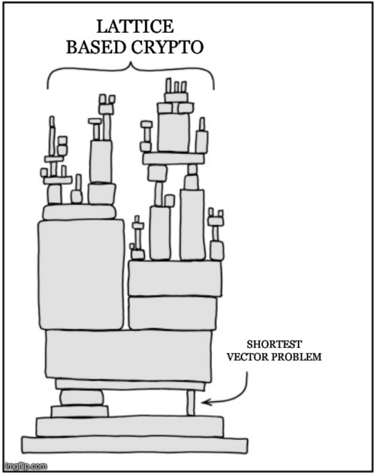
Lattice Isomorphism Problem



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/DSA were both elected by NIST as schemes for standardisation, with the standards published August 2024[a][b]. 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

Slide Title

Section Title Examples

Section Title

Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

Sed et mincipidem am fugia venihitem aut utatem invellupis dolore voluptatiate verior mo dolendi squatur?

Section Title

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

Slide Title

List Examples

Bullet List

- Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?
- Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?
    - Second level indented list item.
        - Third level indented list item.
- Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

Numbered List

1. Sed et mincipidem am fugia venihitem aut utatem invellupis dolore voluptatiate verior mo dolendi squatur?
2. Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?
    a. Second level indented list item.
        i. Third level indented list item.
3. Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

Slide Title

Three-Column Example

Section Title

Sed et mincipidem am fugia ve nihi aut utatem invellupis dore voluptatiate veor olendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur? Pa cumquat ute nos exero magnime officatem. Luptia

Section Title

Sed et mincipidem am fugia ve nihi aut utatem invellupis dore voluptatiate veor olendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur? Pa cumquat ute nos exero magnime officatem. Luptia

Section Title

Sed et mincipidem am fugia ve nihi aut utatem invellupis dore voluptatiate veor olendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur? Pa cumquat ute nos exero magnime officatem. Luptia

Slide Title

Three-Column With Images Example

Section Title

Sed et mincipidem am fugia ve nihi aut utatem invellupis dore voluptatiate veor olendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit?

Section Title

Sed et mincipidem am fugia ve nihi aut utatem invellupis dore voluptatiate veor olendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit?

Section Title

Sed et mincipidem am fugia ve nihi aut utatem invellupis dore voluptatiate veor olendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit?

Slide Title

Large Right Image Example

Section Title

Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

(Above) Photography Credit or Caption

(Above) Photography Credit or Caption

Section Title

Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

Section Title

Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

Pa cumquat ute nos exero magnime officatem. Luptia voluptatur aut acia comnist qui beatusam, omniatecae iur alit, cus debis

(Above) Photography Credit or Caption

Text can be included on slides with image backgrounds too.

Slide Title

Tiled Images Example

Section Title

Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

Slide Title

Tiled Images Example

Section Title

Sed et mincipidem am fugia venihi aut utatem invellupis dolore voluptatiate veor mo dolendi squatur?

Ab illate sitate explibus reiundusam, voluptur sim idebit, omnis dero quas adio quatur?

IMPERIAL

IMPERIAL

IMPERIAL

IMPERIAL

Thank you

IMPERIAL

Thank you.
Questions?

On the subject of lattices
2024-03-22