IMPERIAL

On the subject of lattices

and why cryptographers love them

Joshua Limbrey
2024-03-22

Agenda

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.

[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.

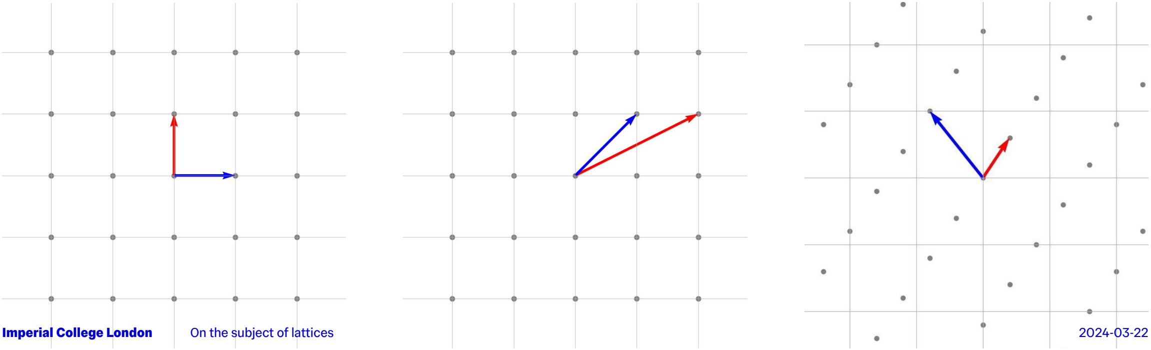
(Above) Cryptographers wanting new toys, circa 2000 (colourised)

What is a lattice?

Definition: Lattice

The set of all linear integer combinations of basis vectors,

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



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)

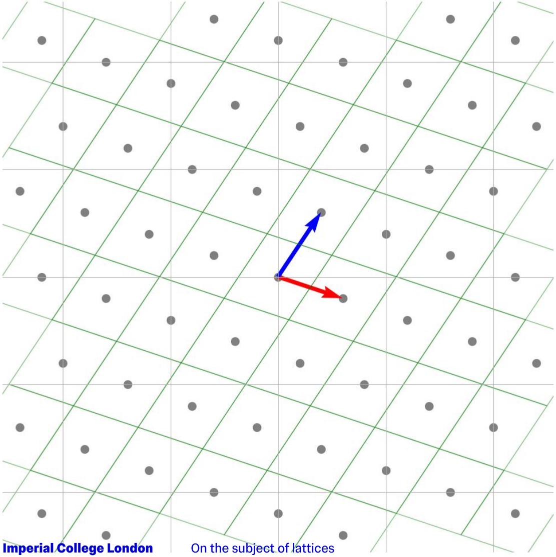
Let, $\begin{bmatrix} \mathbf{b} \end{bmatrix} = \begin{bmatrix} \quad \mathbf{A} \quad \end{bmatrix} \begin{bmatrix} \mathbf{s} \end{bmatrix} + \begin{bmatrix} \mathbf{e} \end{bmatrix}$. Knowing *only* the values in green, find $\begin{bmatrix} \mathbf{s} \end{bmatrix}$.

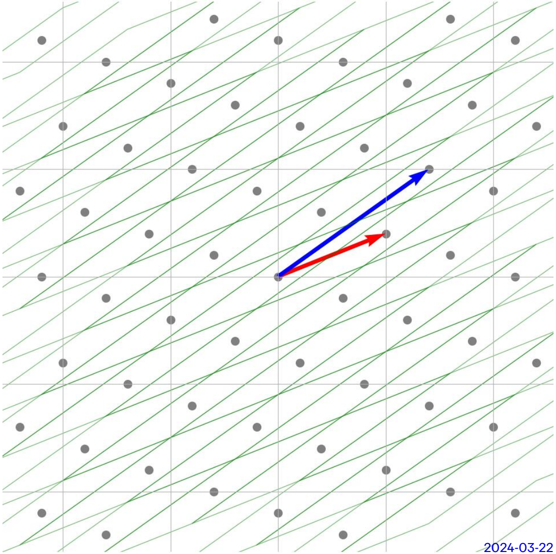
Definition: Lattice Isomorphism Problem (LIP)

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!

Shortest/Closest Vector Problem



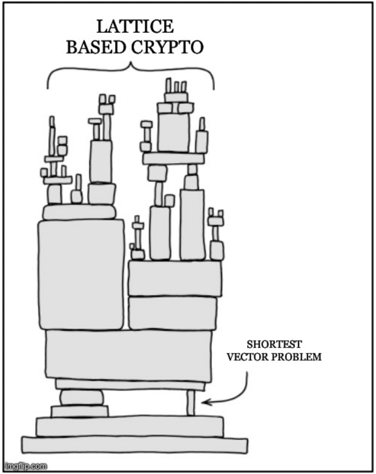


(Above) Cryptographers wanting new toys, circa 2000 (colourised)

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.) We also believe that SVP is a *very* hard problem, even for quantum computers.



(Above) xkcd Dependency, lattice based cryptography special edition

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?