Learning With Errors

Introduction to Homomorphic Cryptosystems – Lecture 2

Learning Without Errors

Solve for $\boldsymbol{x_1, \ldots, x_4}$:

$$34x_1 + 2x_2 + 4x_3 + 67x_4 = 5297$$
$$6x_1 + 25x_2 + 71x_3 + 33x_4 = 6439$$
$$42x_1 + 88x_2 + 64x_3 + 52x_4 = 8790$$
$$13x_1 + 9x_2 + 93x_3 + 49x_4 = 8454$$

No problem using the tools of linear algebra:

$$x = \begin{pmatrix} 5 \\ 18 \\ 50 \\ 73 \end{pmatrix}$$

Adding Error

Let‘s add a random secret error:

$$34x_1 + 2x_2 + 4x_3 + 67x_4 = 5297 - 4$$
$$6x_1 + 25x_2 + 71x_3 + 33x_4 = 6439 + 1$$
$$42x_1 + 88x_2 + 64x_3 + 52x_4 = 8790 + 3$$
$$13x_1 + 9x_2 + 93x_3 + 49x_4 = 8454 - 2$$

Which gives us these equations:

$$34x_1 + 2x_2 + 4x_3 + 67x_4 = 5293$$
$$6x_1 + 25x_2 + 71x_3 + 33x_4 = 6440$$
$$42x_1 + 88x_2 + 64x_3 + 52x_4 = 8793$$
$$13x_1 + 9x_2 + 93x_3 + 49x_4 = 8452$$

Now solve for $x_1, \dots, x_4$

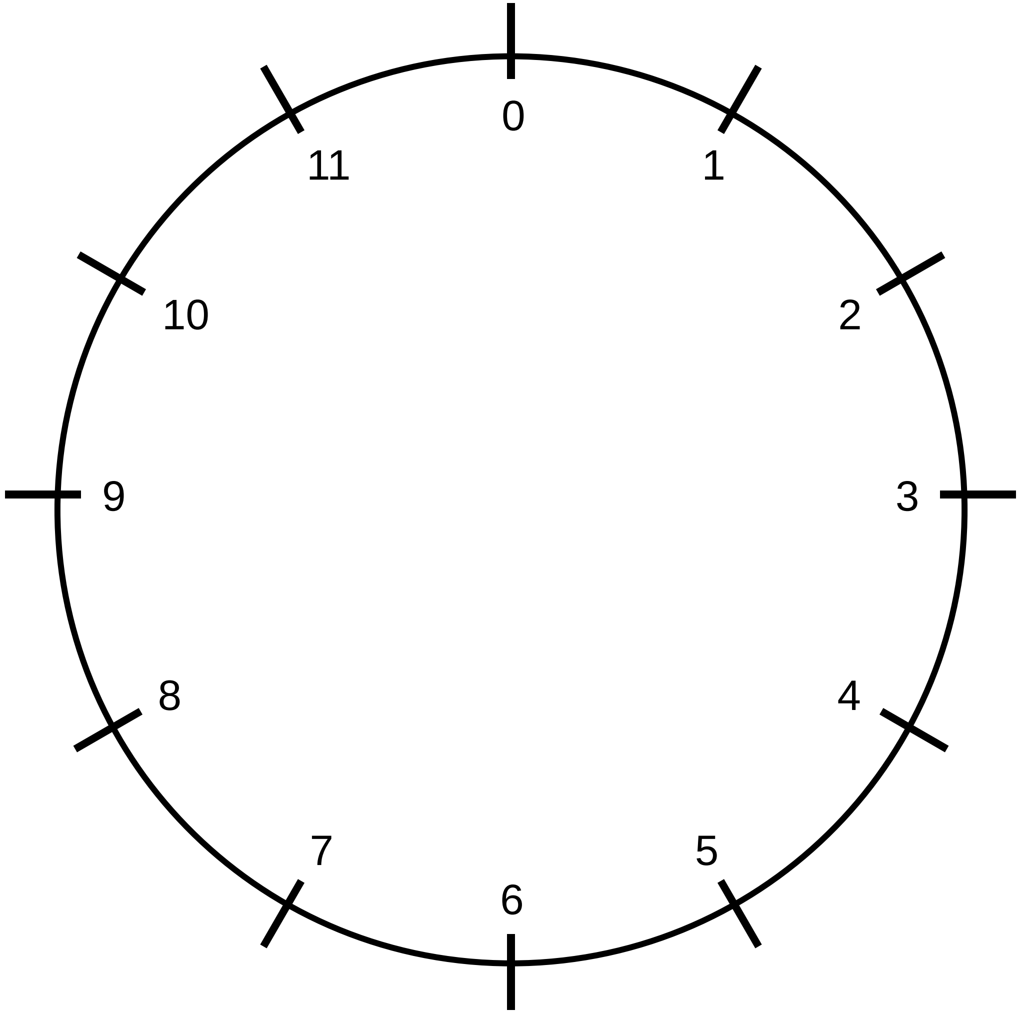
➡ much more difficult

MODULAR ARITHMETIC

Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers.
The numbers “wrap around” when reaching a certain value, called **modulus.**

Example: 12-hour clock



Modular Arithmetic

Congruence

Given an integer $m \geq 1$, two integers a, b are congruent modulo m if there is an integer k such that

$$a - b = km$$

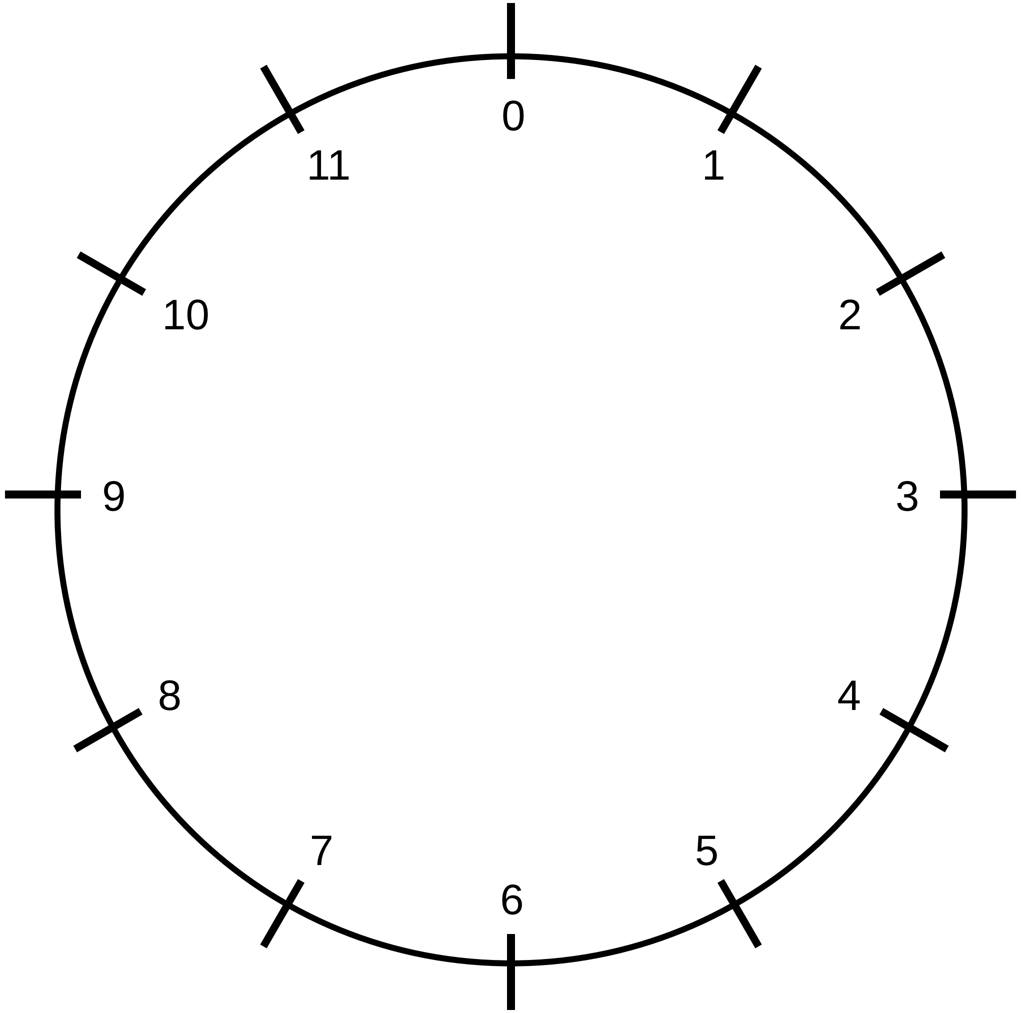
You can write this relation as:

$$a \equiv b \pmod{m}$$

Example

$5 \equiv 17 \pmod{12}$, because

$$5 - 17 = -12 = -1 * 12$$

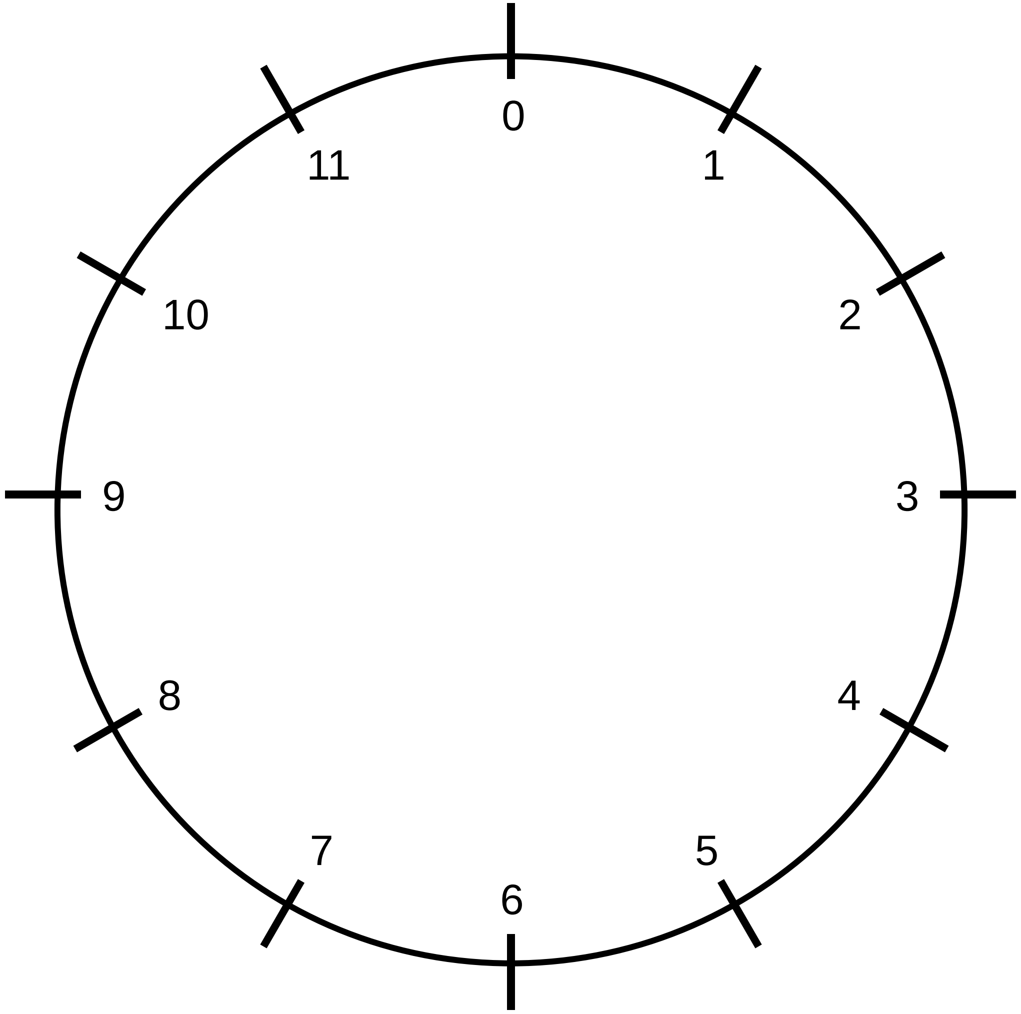


Modular Arithmetic

Congruence classes
The set of all integers of the form

$$a + km$$

is called the congruence class (or residue class) of a modulo m.



Notation

$$(a \bmod m)$$
$$\bar{a}_m$$
$$[a]_m$$

Example

$$\bar{4}_{12} = \{4, 16, 28, 40, \dots\}$$

Modular Arithmetic

Integers modulo m
The set of all congruence classes modulo m is called the ring of integers modulo m.

Notation

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{a}_m | a \in \mathbb{Z}\} = \{\bar{0}_m, \bar{1}_m, \bar{2}_m, \dots, \overline{m-1}_m\}$$

More on that in future lectures!

LWE DEFINITION

Learning with Errors

$a_1 = (34,2,4,67)^\perp$
$a_2 = (6,25,71,33)^\perp$
$a_3 = (42,88,64,52)^\perp$
$a_4 = (13,9,93,49)^\perp$

$b_1 = \langle s, a_1 \rangle + e_1$
$b_2 = \langle s, a_2 \rangle + e_2$
$b_3 = \langle s, a_3 \rangle + e_3$
$b_4 = \langle s, a_4 \rangle + e_4$

$$34x_1 + 2x_2 + 4x_3 + 67x_4 = 5297 - 4$$
$$6x_1 + 25x_2 + 71x_3 + 33x_4 = 6439 + 1$$
$$42x_1 + 88x_2 + 64x_3 + 52x_4 = 8790 + 3$$
$$13x_1 + 9x_2 + 93x_3 + 49x_4 = 8454 - 2$$

$e = (e_1, e_2, e_3, e_4)^\perp = (-4,1,3,-2)^\perp$

Learning with Errors

$\mathbb{Z}_q^n$ = n-dimensional integer vectors modulo q

$\langle v, w \rangle \coloneqq$ inner product of the vectors v, w

$\langle v, w \rangle \coloneqq \sum_{i=1}^{n} v_i, w_i$

Parameters
dimension $\boldsymbol{n}$
modulus $\boldsymbol{q} = \mathrm{poly}(n)$
error distribution $\boldsymbol{\chi}$

$\mathrm{a}_1 \leftarrow \mathbb{Z}_q^n, \quad b_1 = \langle s, a_1 \rangle + \mathrm{e}_1 \in \mathbb{Z}_q$

$\mathrm{a}_2 \leftarrow \mathbb{Z}_q^n, \quad b_2 = \langle s, a_2 \rangle + \mathrm{e}_2 \in \mathbb{Z}_q$

...

uniform random

$\mathbb{Z}_q$ = integers modulo q

$$\mathbf{A} = \begin{pmatrix} | & | & \\ a_1 & a_2 & \dots \\ | & | & \end{pmatrix}$$

$$\boldsymbol{b}^{\perp} = (b_1, b_2, \dots) \approx \boldsymbol{s}^T A$$

Search Problem
Find secret $s \in \mathbb{Z}_q^n$ given
$\mathbf{A}$ and $\boldsymbol{b}^{\perp} \approx \boldsymbol{s}^{\perp}\boldsymbol{A}$

Decision Problem
Distinguish $(\boldsymbol{A}, \boldsymbol{b})$ from uniform $(\boldsymbol{A}, \boldsymbol{b})$

BUILD A CRYPTOSYSTEM FROM THE LWE PROBLEM

Symmetric vs Antisymmetric Cryptosystem

Symmetric cryptosystem
There is one key shared with both parties. The key is used to encrypt the data.

Advantages
Simple, easy to implement and calculate

Disadvantages
Key has to be shared between the parties

Antisymmetric cryptosystem
Every party has two keys (public and private key). Messages encrypted with the public key can be decrypted with the private key.

Advantages
The public key can be shared without a problem as it can be only used for encryption

Disadvantages
More complex calculations.
Security comes from the assumption, that it is hard to get the private key from the public key

A Symmetric LWE Cryptosystem

Encryption
choose
$\boldsymbol{s}^T = (s_0, \ldots, s_{n-1}) \in \{0,1\}^n$
$\boldsymbol{a}^\mathrm{T} = (\mathrm{a}_0, \ldots, \mathrm{a}_{\mathrm{n}-1}) \in \mathbb{Z}_q^n$

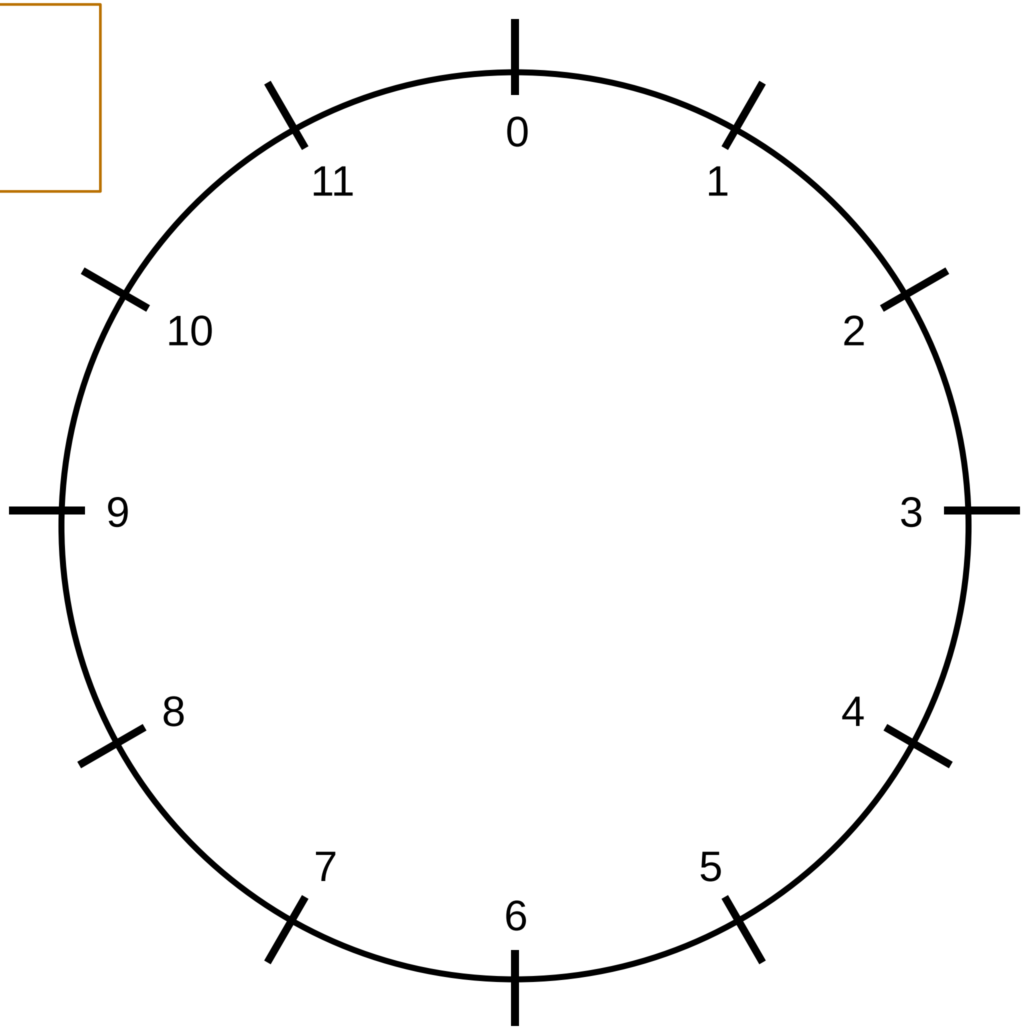
bit
modular integer
real in an interval

Encryption of a message m:

$Enc(m) = (a_0, \ldots, a_{n-1}, b) = (\boldsymbol{a}^T, b) = c$
where
$b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e + Encoding(m)$

drawn from error distribution. This the LWE definition and provides security

Decryption
$Dec(c) = b - \langle \boldsymbol{a}, \boldsymbol{s} \rangle = Encoding(m) + e$



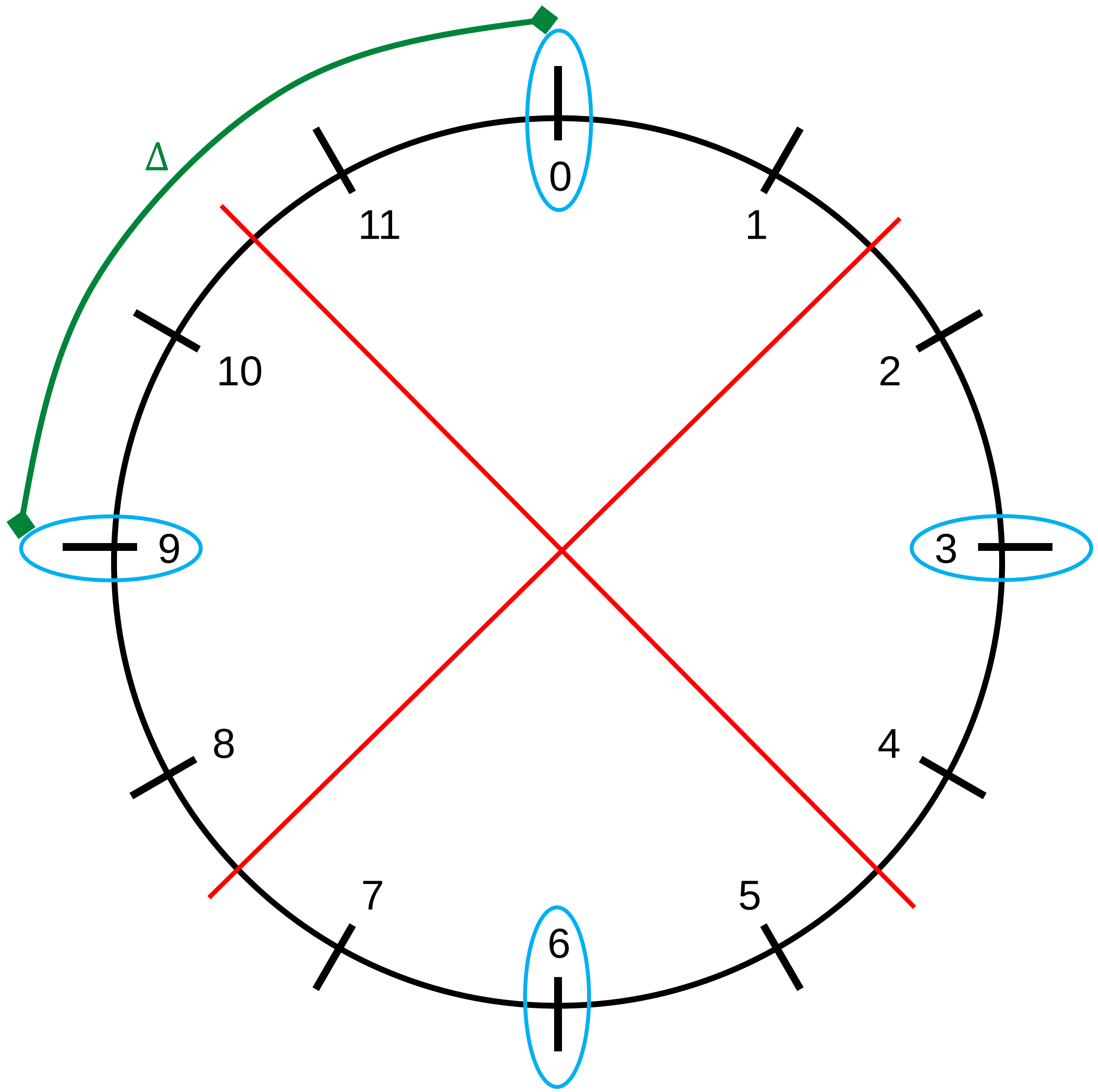
https://www.zama.ai/post/tfhe-deep-dive-part-1

Encoding and Error

Parameters
modulus $q = 12$
number of different messages $p = 4$
set of possible messages $\mathcal{M} = \{0,1,2,3\}$
'distance' between messages $\Delta = \frac{q}{p} = 3$

Encoding
We choose a message $m \in \mathcal{M}$
$Encoding(m) = m * \Delta$
This scales the message to leave enough place for the error but is no encryption!

Error
must be in the range Δ around the encoded message
$|e| < \frac{\Delta}{2} = 1{,}5$



https://www.zama.ai/post/tfhe-deep-dive-part-1

Encoding and Error: Example

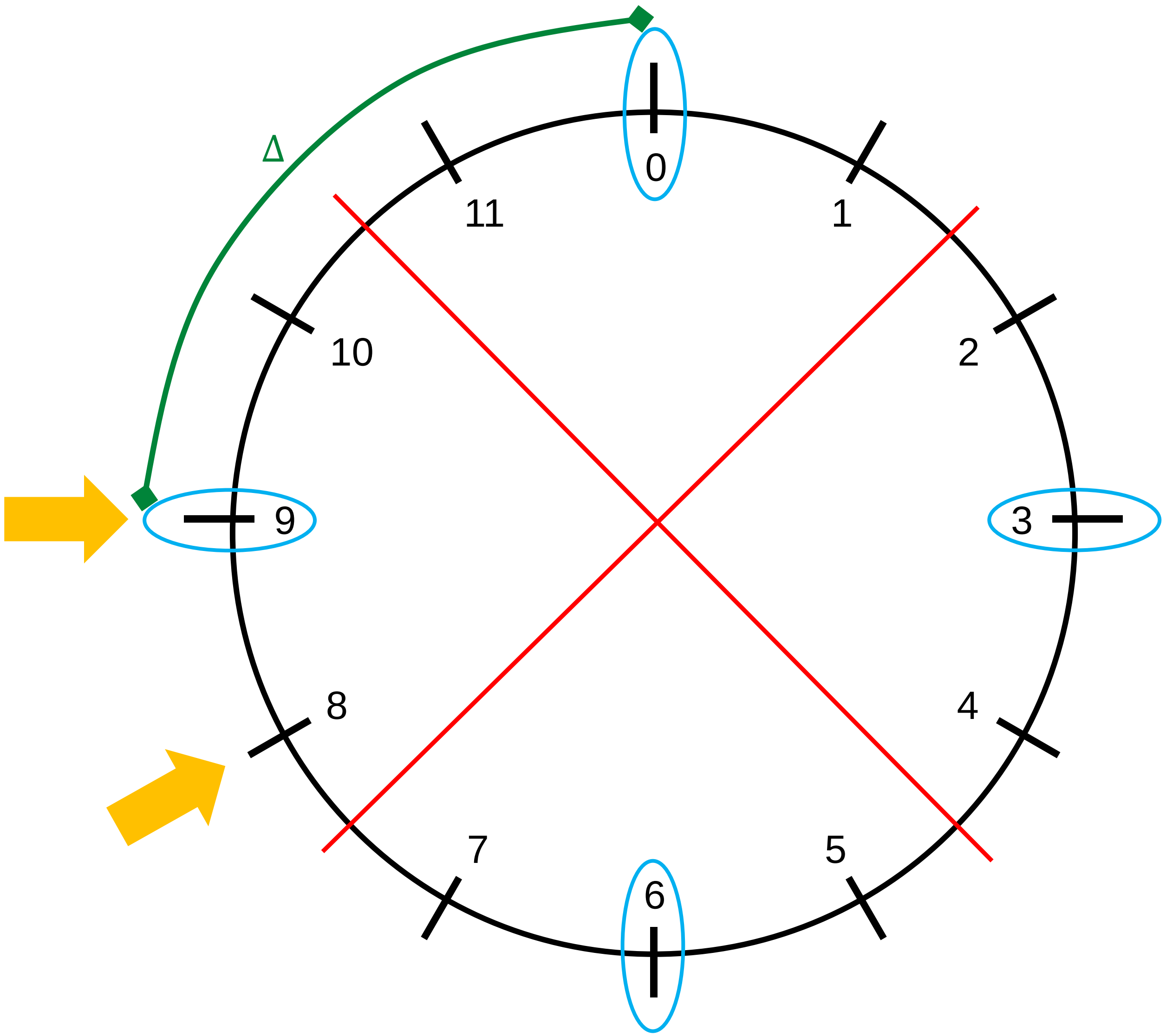
Example

We want to send the message $m = 3$

$Encoding(m) = 9$

We draw the error $e = -1$

$Encoding(m) + e = 8$



https://www.zama.ai/post/tfhe-deep-dive-part-1

Homomorphic Properties of the Symmetric Cryptosystem

Take two encrypted messages:

$Enc(m) = \left(\boldsymbol{a}^{\mathrm{T}}, b\right) = c$ $\qquad b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e + \Delta m$

$Enc(m') = \left(\boldsymbol{a}'^{\mathrm{T}}, b'\right) = c'$ $\qquad b' = \langle \boldsymbol{a}', \boldsymbol{s} \rangle + e + \Delta m'$

$Dec(c) = b - \langle \boldsymbol{a}, \boldsymbol{s} \rangle$

The inner product is distributive over vector addition

$\langle \boldsymbol{a} + \boldsymbol{b}, \boldsymbol{c} \rangle = \langle \boldsymbol{a}, \boldsymbol{c} \rangle + \langle \boldsymbol{b}, \boldsymbol{c} \rangle$

Addition

$Dec(c + c') = Dec\big((\boldsymbol{a}^T + \boldsymbol{a}'^T, b + b')\big) = b + b' - \langle \boldsymbol{a} + \boldsymbol{a}', \boldsymbol{s} \rangle =$

$= \langle \boldsymbol{a}, \boldsymbol{s} \rangle + \langle \boldsymbol{a}', \boldsymbol{s} \rangle - \langle \boldsymbol{a} + \boldsymbol{a}', \boldsymbol{s} \rangle + 2e + \Delta(m + m') = 2e + \Delta(m + m')$

The error increases!

Constant Multiplication

$Dec(\gamma * c) = Dec\big((\gamma * \boldsymbol{a}, \gamma * b)\big) = \gamma * b - \langle \gamma * \boldsymbol{a}, \boldsymbol{s} \rangle =$

$= \gamma * \langle \boldsymbol{a}, \boldsymbol{s} \rangle - \langle \gamma * \boldsymbol{a}, \boldsymbol{s} \rangle + \gamma * e + \gamma * \Delta m = \gamma e + \Delta \gamma m$

The error increases!

$\in \mathbb{Z}$

Public-Key Cryptosystem from LWE

public parameter

$A \leftarrow \mathbb{Z}_q^{n\times m}$

Alice

chooses vector $\boldsymbol{x}$

secret key

Bob

$\boldsymbol{s} \leftarrow \mathbb{Z}_q^{n}$

$\boldsymbol{u} = \boldsymbol{A}\boldsymbol{x}$

(public key, uniform when $m > n \log q$)

LWE problem, this provides security

$\boldsymbol{b}^T = \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T$

(ciphertext 'preamble')

When all parameters are set correctly

$b' - \boldsymbol{b}^T\boldsymbol{x} \approx bit * \frac{q}{2}$

$b' = \boldsymbol{s}^T\boldsymbol{u} + e + \text{bit} * \frac{q}{2}$

('payload')

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. 2008. Trapdoors for hard lattices and new cryptographic constructions.

Public-Key Cryptosystem from LWE

Alice
chooses vector $\boldsymbol{x}$

$\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$

Bob
$\boldsymbol{s} \leftarrow \mathbb{Z}_q^{n}$

Eve
can observe
$\boldsymbol{A}\ \boldsymbol{u}\ \boldsymbol{b}\ b'$

But according to the LWE problem, she cannot distinguish between
$(\boldsymbol{A}, \boldsymbol{u}), (\boldsymbol{b}, b')$
and uniform
$(\boldsymbol{A}, \boldsymbol{u}), (\boldsymbol{b}, b')$

$\boldsymbol{u} = \boldsymbol{A}\boldsymbol{x}$
(public key, uniform when $m > n \log q$)

$\boldsymbol{b}^T = \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T$
(ciphertext ‘preamble’)

$b' = \boldsymbol{s}^T\boldsymbol{u} + e + \mathrm{bit} * \frac{q}{2}$
(’payload’)

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. 2008. Trapdoors for hard lattices and new cryptographic constructions.

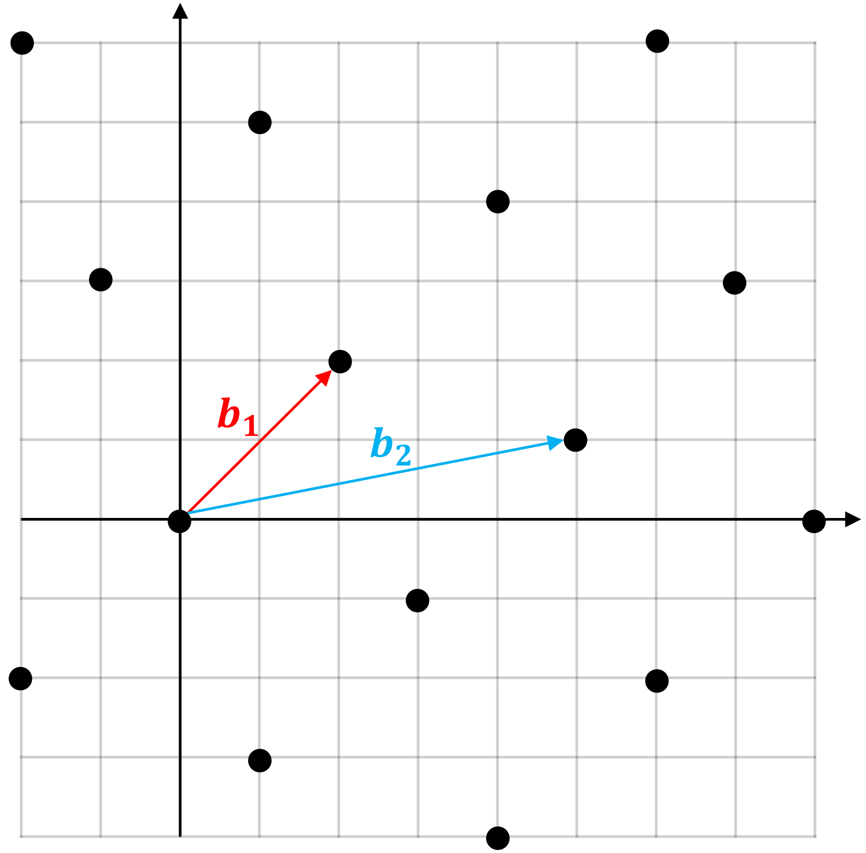
LATTICE PROBLEMS

What is a Lattice?

A **lattice** in the real coordinate space $\mathbb{R}^n$ is an infinite set of points (or vectors).

Properties:

- Coordinate-wise addition or subtraction of two points in the lattice produce another lattice point
- All lattice points are separated by some minimum distance



Mathematical definition
Let $\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots, \boldsymbol{b_m}$ be linearly independent vectors in $\mathbb{R}^n$.

$$L \ := \{\sum_{i=1}^{m} g_i \boldsymbol{b_i} \,|g_i \in \mathbb{Z}\}$$

is called a lattice with basis $B = \{b_1, b_2, \ldots, b_m\}$.

The length of the shortest non-zero vector in the lattice L is defined as

$$\lambda(L) = \min_{\boldsymbol{x} \in L \setminus \{0\}} ||\boldsymbol{x}||_N$$

What is a Lattice?

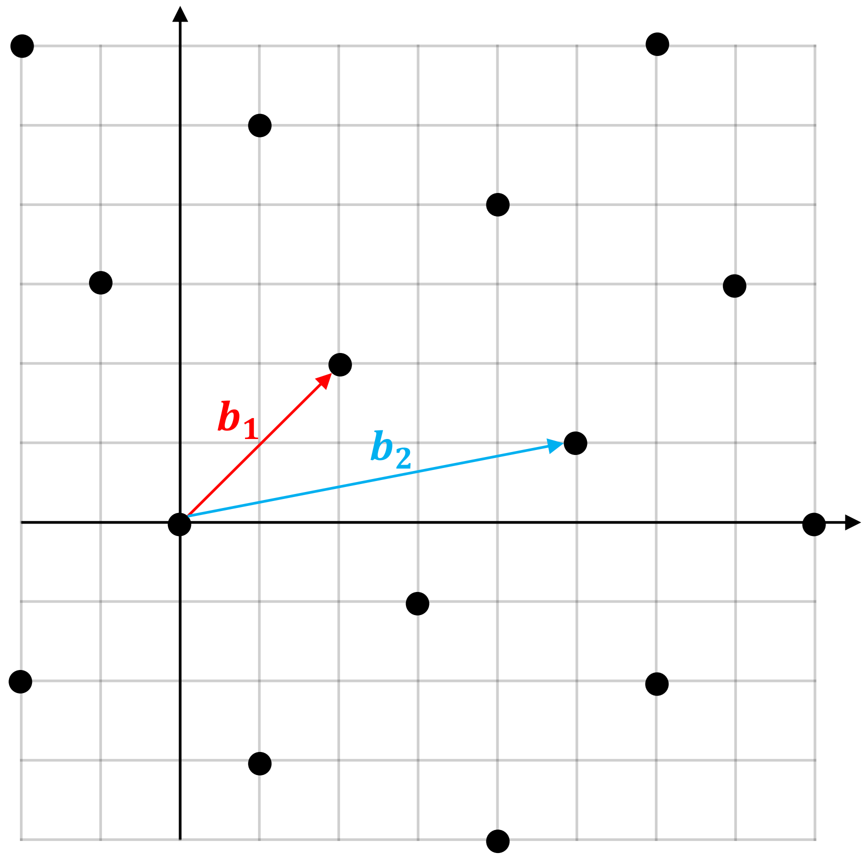
The operation of the group is also commutative:

$$x + y = y + x$$

Mathematical description

A lattice is a free abelian group of dimension n which spans the vector space $\mathbb{R}^n$.

A free group has a basis B with the property, that every element of the group can be uniquely expressed as a linear combination of finite many basis elements.



Other Examples

The following groups are also free abelian groups

- $(\mathbb{Z}, +)$ with $B = \{1\}$
- $(\mathbb{Q}^+, *)$ with the prime numbers as B

Positive rational numbers

Shortest Vector Problem (SVP)

Parameters

A basis B which defines a lattice L

Norm N (usually the Euclidean norm)

Problem

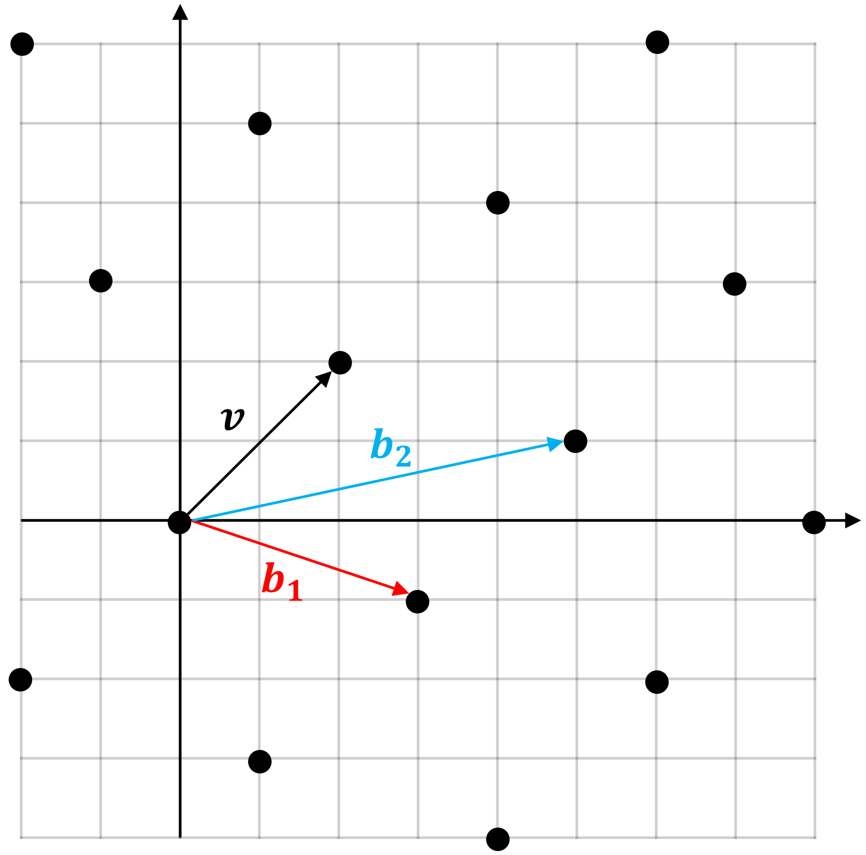
Find a non-zero vector $\boldsymbol{v} \in L$ such that

$$\left|\left|\boldsymbol{v}\right|\right|_N = \lambda(L)$$

GapSVP

Given β, which can be a fixed function of the dimension of the lattice, decide whether

$$\lambda(L) \leq 1 \text{ or } \lambda(L) > \beta$$



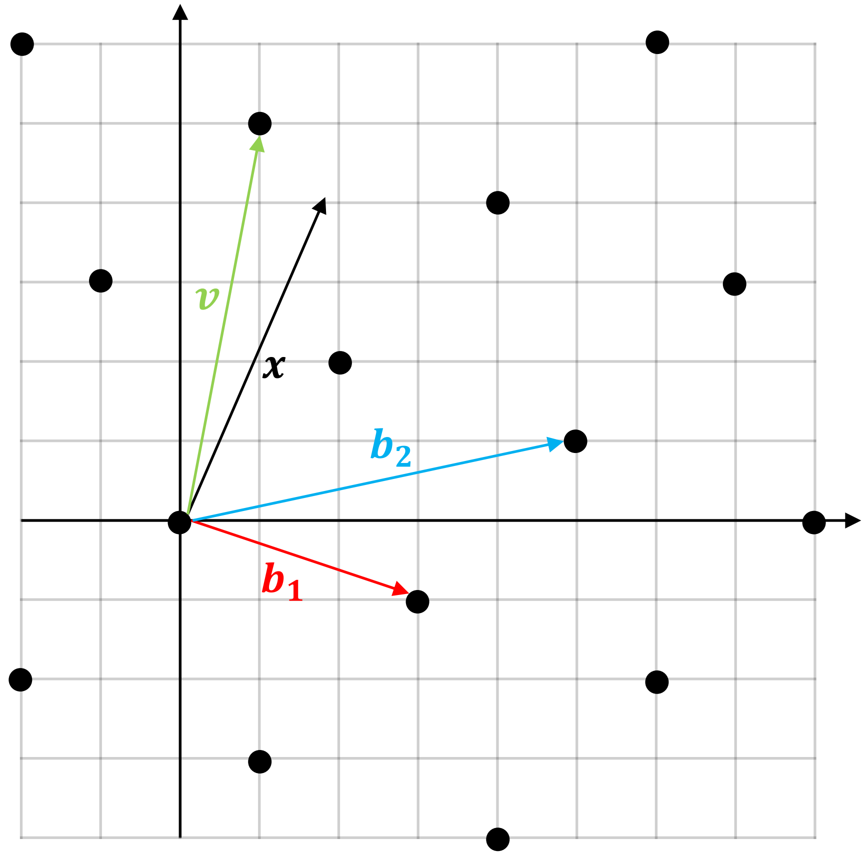
Closest Vector Problem (CVP)

Parameters

A basis B of a vector space V which defines a lattice L
Metric M (usually the Euclidean norm)
Vector $\boldsymbol{x} \in V$

Problem

Find the vector $\boldsymbol{v} \in L$ closest to $\boldsymbol{x}$ (as measured by M).



GapCVP

Given β, which can be a fixed function of the dimension of the lattice, decide whether

- there is a lattice vector such that the distance between it and $\boldsymbol{x}$ is at most 1, or
- every lattice vector is at a distance greater than β away from $\boldsymbol{x}$.

LWE is a Lattice Problem

Reminder LWE Definition

$a_1 \leftarrow \mathbb{Z}_q^n$, $\quad b_1 = \langle s, a_1 \rangle + e_1 \in \mathbb{Z}_q$

$a_2 \leftarrow \mathbb{Z}_q^n$, $\quad b_2 = \langle s, a_2 \rangle + e_2 \in \mathbb{Z}_q$

…

$$\boldsymbol{A} = \begin{pmatrix} | & | & \\ a_1 & a_2 & \dots \\ | & | & \end{pmatrix}$$

$$\boldsymbol{b}^T = (b_1, b_2, \dots) \approx s^t A$$

LWE lattice

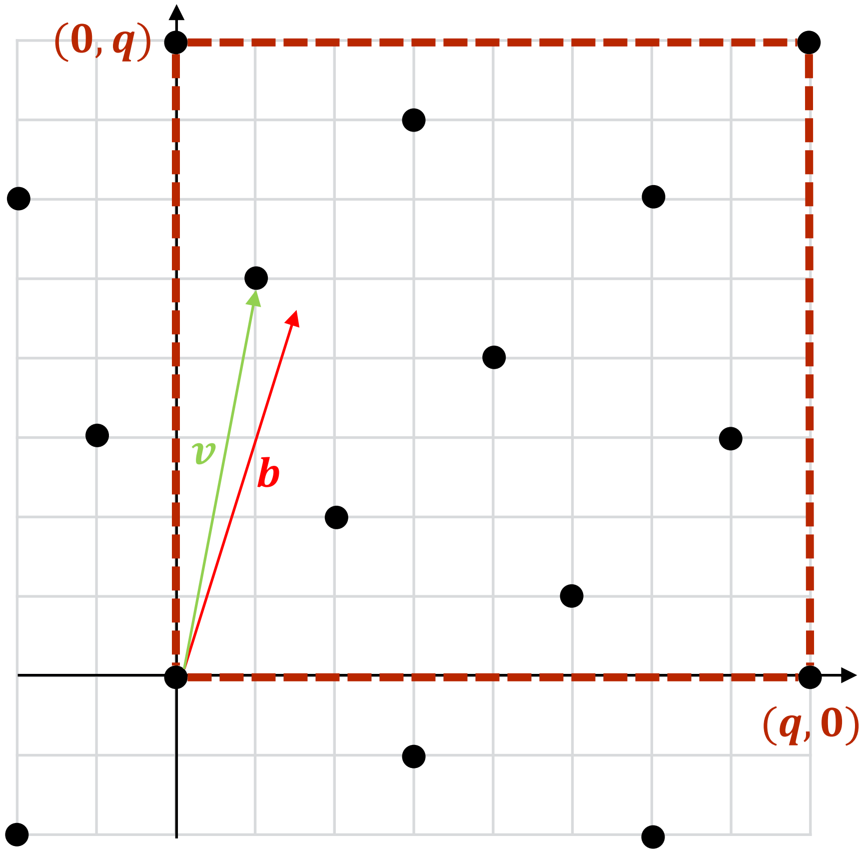
$$L(\boldsymbol{A}) = \{\boldsymbol{z} \in \mathbb{Z}^m | \boldsymbol{z}^T \equiv \boldsymbol{s}^T \boldsymbol{A} \bmod q\}$$

LWE as a lattice problem

Given $L(\boldsymbol{A})$ and $\boldsymbol{b}^T \approx \boldsymbol{v}^T = \boldsymbol{s}^T \boldsymbol{A} \in \boldsymbol{L}(\boldsymbol{A})$, find $\boldsymbol{v}$.

$\boldsymbol{b}$ is guaranteed to be 'very close' to a lattice point, which makes LWE a bounded distance decoding problem

Similar to CVP, but the distance from the given vector to the lattice is at most $\lambda(L)/2$



Lattice Problems in Cryptography

- SVP, CVP and LWE are all in the same category of hardness (NP-hard)
- No efficient (quantum-) algorithms are known for lattice related problems
- Lattice based cryptosystems are often algorithmically simple and highly parallelizable
  - Mainly linear operations on vectors
  - Matrices modulo small integers
- Famous lattice-based schemes
  - NTRUEncrypt
  - Kyber
  - TFHE

LWE is the base problem for (almost) every HE cryptosystem!

Summary – What did we learn today?

LWE

What is the learning with errors problem?

The LWE problem is the challenge to find the solution to a linear system of equations, which is altered by a small error.

We can build symmetric and public key cryptosystems based on LWE.

Modular arithmetic

In modular arithmetic the numbers 'wrap around' when reaching a certain modulus.

$a \equiv b \pmod{m}$ tells us that a and b have the same remainder when divided by m.

Lattice Problems

Shortest Vector Problem (SVP)

Closest Vector Problem (CVP)

LWE is also a lattice problem and therefore as hard to solve.

Lattice-based cryptography seems to be a solution for the post-quantum era.