# Lattice Cryptography!

(Notes inspired by David Wu / Florian Tramer)

## Course Overview

| Foundations | ECC | MPC | Lattices |
|---|---|---|---|
| PRGs | Sigma | OT | ⋮ |
| PRFS | Pairings | Garbled Circuits | |
| PRPs | ZK | 2-PC Beaver Triples | |
| Commits | ⋮ | | |

Amazing stuff, what else could there be?

## Lattice Based Cryptography

For example, dLog + factoring are much easier with quantum computers

- Plausibly Post Quantum: We need to update our primitives/protocols to be secure against adversaries that have quantum computers

Same organization that standardized AES

- NIST Post Quantum Standardization Finalists

  Signature Schemes
  - Lattice based: Dilithium, Falcon
  - Hash based: SPHINCS

  Code based KEMs are still being considered.

  Key Encapsulation Mechanisms
  - Lattice based: Kyber

Isogeny Candidates broken

- Diversify cryptographic assumptions for primitives
    - opens potential avenues to base cryptography on worst case hardness / holy grail: cryptography based on NP-hard problems

normally rely on avg case hardness

- Enables new functionalities!!!
    - Fully Homomorphic Enc: Given an enc of a message $x$, noninteractively and efficiently compute a valid enc of $f(x)$ for any function $f$ (of polysize)

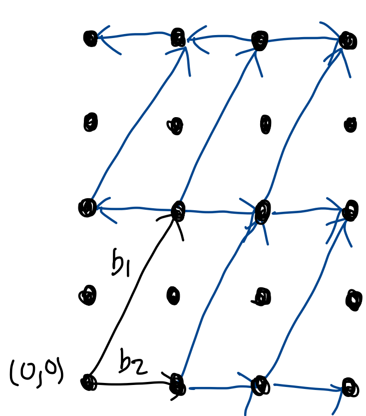
but... What is a Lattice?

__Def__: An n-dimensional lattice $\mathcal{L}$ is a "discrete, additive subspace" of $\mathbb{R}^n$.

- __Discrete__: every $x \in \mathcal{L}$ has a neighborhood in $\mathbb{R}^n$ where it is the __only__ point.
- __Additive subspace__: $0^n \in \mathcal{L}$ and $\forall x, y \in \mathcal{L}$, $-x \in \mathcal{L}$ and $x+y \in \mathcal{L}$

__Example__: the integer lattice $\mathbb{Z}^n$. the $q$-ary lattice $q\mathbb{Z}^n$ (i.e. the set of vectors whose entries are multiples of $q$)

__Picture__:



## Computational Problems:

- Shortest Vector Problem: given a basis $B$ for a lattice $\mathcal{L}(B)$, find the shortest non-zero vector $v \in \mathcal{L}(B)$
- Approximate SVP: SVP but with an approximation factor
- Decision problems and many more...

Today, we will discuss the LWE Assumption and construct PKE from it.

**Def:** The Learning with Errors (LWE) problem is defined with respect to lattice parameters $n, m, q$ and an error distribution $\chi_B$ (often, a discrete Gaussian distribution over $\mathbb{Z}_q$). The LWE assumption states that for random $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, $s \xleftarrow{\$} \mathbb{Z}_q^n$, $e \leftarrow \chi_B^m$, the two dists

$$\left\{ (A, As+e) : \begin{array}{l} A \xleftarrow{\$} \mathbb{Z}_q^{m\times n} \\ s \xleftarrow{\$} \mathbb{Z}_q^n \\ e \leftarrow \chi_B^m \end{array} \right\} \approx \left\{ (A, r) : \begin{array}{l} A \xleftarrow{\$} \mathbb{Z}_q^{m\times n} \\ r \xleftarrow{\$} \mathbb{Z}_q^m \end{array} \right\}$$

are computationally indistinguishable.

☆ LWE viewed as a lattice problem

- $\mathcal{L}(A) = \{ As : s \in \mathbb{Z}_q^n \} + q\mathbb{Z}^n$
- The search version of LWE: find $s$ given $As+e$ can be reformulated as: given a point $As+e$ near a lattice point $p \in \mathcal{L}$, find $p \iff$ finding $s$.

# Why does LWE seem hard? (detour to search variant)

☆ the search and decision variants of LWE are $\approx$ equally hard!

Lets remove the error for a moment:

$$\left[ A \in \mathbb{Z}_q^{m \times n} \right] \left[ s \in \mathbb{Z}_q^n \right] = \left[ b \in \mathbb{Z}_q^m \right]$$

$m$ equations, $n$ unknowns if $m \geq n$ can use gaussian elimination to solve the linear system.

Adding back error:

$$\left[ A \in \mathbb{Z}_q^{m \times n} \right] \left[ s \in \mathbb{Z}_q^n \right] \underset{\uparrow}{\simeq} \left[ b \in \mathbb{Z}_q^m \right] + \left[ e \leftarrow \chi_B^m \right]$$

noisy, not equality!

Have to solve a noisy linear system of equations.

For some choices of parameters and noise distributions, we believe this problem is both well defined / hard.

- $n$ = security parameter (more unknowns = harder system)
- $m = \text{poly}(n)$, $m \gg n$ (overdetermined) (more equations = easier problem)
- $q = \text{poly}(n)$
- $B \ll q$ in $\chi_B$ is a noise bound. All $e$ in the support of $\chi_B$ have $\|e\|_\infty \leq B$. (less noise = easier problem)

$\|e\|_\infty = \max_{i \in [m]} (|e_i|)$

# Regev Encryption (2005)

A simple "EL-Gamal style" public key cryptosystem from LWE.

★ Note: - We will view $\mathbb{Z}_q$ as integers in range $(-\frac{q}{2}, \frac{q}{2})$
for example $\mathbb{Z}_7 := \{-3, -2, -1, 0, 1, 2, 3\}$
- $\lfloor \cdot \rfloor$ : floor will round down to nearest integer

## KeyGen$(1^\lambda)$:

$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, $s \xleftarrow{\$} \mathbb{Z}_q^n$, $e \leftarrow \chi_B^m$

$b := As + e \in \mathbb{Z}_q^m$

Output $(sk := s, pk := (A, b))$

must choose params s.t. $q/4 > mB$ for correctness

## Encrypt$(pk, x \in \{0,1\})$:

encrypts single bits... large ciphertexts

$r \xleftarrow{\$} \{0,1\}^m$, $c_0 := r^T A \in \mathbb{Z}_q^n$, $c_1 := r^T b + \lfloor \frac{q}{2} \rfloor \cdot x$

Output $ct := (c_0, c_1) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

## Decrypt$(sk := s \in \mathbb{Z}_q^n, ct := (c_0, c_1))$:

$\tilde{x} := c_1 - c_0 \cdot s$

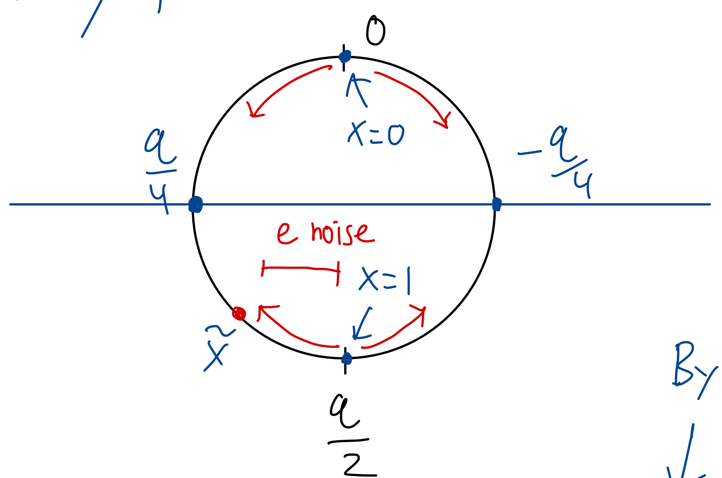
if $|\tilde{x}| < q/4$ output 0

else output 1

## Correctness:

$$\tilde{x} = c_1 - c_0 \cdot s = r^T b + \lfloor \tfrac{q}{2} \rfloor \cdot x - r^T A s$$
$$= r^T (As + e) + \lfloor \tfrac{q}{2} \rfloor x - r^T A s$$
$$= \cancel{r^T A s} + r^T e + \lfloor \tfrac{q}{2} \rfloor x - \cancel{r^T A s}$$
$$= \underbrace{r^T e + \lfloor \tfrac{q}{2} \rfloor \cdot x}_{\text{noisy plaintext}}$$

Visual Interpretation:




By choice of params

We have $e \leftarrow \chi_B^m$ and $r \xleftarrow{\$} \{0,1\}$ so $|r^T e| \le mB < \frac{q}{4}$

So if $x = 0$, $|\tilde{x}| < \frac{q}{4}$ else if $x = 1$, $|\tilde{x}| > \lfloor \frac{q}{2} \rfloor - \frac{q}{4} \geq \frac{q}{4}$.

## Security (Proof Sketch):

View of Adversary

Hybrid$_0$ : $pk = (A, b = As + e)$, $c_0 = r^T A$, $c_1 = r^T b + \lfloor \frac{q}{2} \rfloor \cdot x$

Comp Ind by LWE $\qquad \approx_c$

Hybrid$_1$ : $pk = (A, v \xleftarrow{\$} \mathbb{Z}_q^m)$, $c_0 = r^T A$, $c_1 = r^T v + \lfloor \frac{q}{2} \rfloor x$

statistically Ind by LHL (next page) $\qquad \approx_s$

Hybrid$_2$ : $pk = (A, v \xleftarrow{\$} \mathbb{Z}_q^m)$, $c_0 \xleftarrow{\$} \mathbb{Z}_q^n$, $c_1 \xleftarrow{\$} \mathbb{Z}_q$

In $\text{Hybrid}_2$, the ciphertext is random and independent of $x$.

**Leftover Hash Lemma (LHL):** ☆ Proof omitted!

- Let $m \geq 2n\log q$.

$$\left\{ (r^T A,\ r^T v) :\ \begin{array}{l} A \xleftarrow{\$} \mathbb{Z}_q^{m\times n} \\ r \xleftarrow{\$} \{0,1\}^m \\ v \xleftarrow{\$} \mathbb{Z}_q^m \end{array} \right\} \approx_s \left\{ (v, w) :\ \begin{array}{l} v \xleftarrow{\$} \mathbb{Z}_q^n \\ w \xleftarrow{\$} \mathbb{Z}_q \end{array} \right\}$$

Therefore,

$$c_0 = r^T A \approx_s c_0 \xleftarrow{\$} \mathbb{Z}_q^n$$

$$c_1 = \underbrace{r^T v + \left\lfloor \frac{q}{2} \right\rfloor \cdot x}_{\text{one time pad}} \approx_s c_1 \xleftarrow{\$} \mathbb{Z}_q$$