Towards Quantum Algorithms for Learning with Errors

Shashwat Agrawal

Learning with Errors

Given a system of linear equations in $\mathbb{Z}_q$: (Make RHS noisy)

$$\begin{pmatrix} & A & \end{pmatrix}_{m \times n} \quad [\,b\,] = As + e$$

secret $s \in \mathbb{Z}_q^n$

noise vector e from a distribution in $\mathbb{Z}_q^m$

Can we find the secret s efficiently (with high probability)?

We can efficiently find

This simple innovation has baffled theorists and thrilled cryptographers

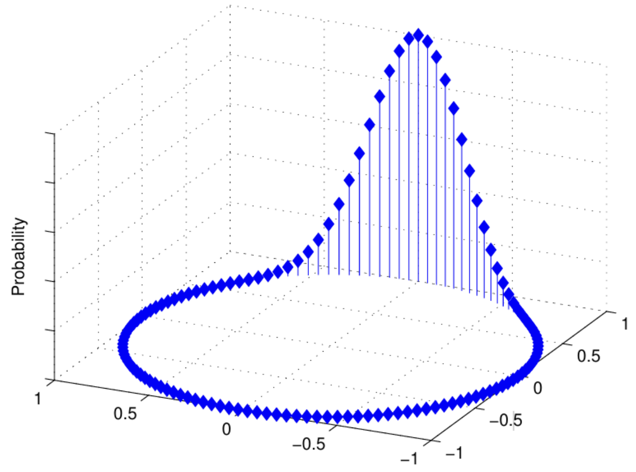
Learning with Errors

Find secret vector s given m vectors along with noisy inner produ

$$a_i \leftarrow \mathbb{Z}_q^n \qquad b_i = \langle s, a_i \rangle + e_i \in \mathbb{Z}_q$$
$$e_i \leftarrow \chi$$

Most popular χ: Discrete Gaussian with variance $\alpha q / \sqrt{2\pi}$

$$A = \begin{pmatrix} - a_i - \end{pmatrix} \quad b = \begin{pmatrix} b_i \end{pmatrix}$$



Discrete Gaussian

Classical Algorithms for LWE

$a_i \leftarrow \mathbb{Z}_q^n$ $b_i = \langle s, a_i \rangle + e_i \in \mathbb{Z}_q$

$e_i \leftarrow \chi$ (Discrete Gaussian with variance $\alpha q / \sqrt{2\pi}$)

- Naïve Algorithm
  - Find a set S of equations $\langle a_i, x \rangle = b_i$ such that $c_i \sum_{i \in S} a_i = (1,0, \dots, 0)$
  - $c_i \sum_{i \in S} b_i$ gives first entry of s. But with probability $\frac{1}{q} + q^{-\Theta(n)}$
  - Repeat $q^{\Theta(n)}$ times for high confidence
- Arora-Ge Algorithm
  - An efficient time algorithm when noise is sufficiently concentrated.
  - When $\|e_i\| \leq d$ and q is sufficiently large, it takes $\exp\left(\tilde{O}(d^2)\right)$ time

No known sub-exponential or arbitrary small exponential time algorithm for $\alpha q = \Omega(\sqrt{n})$

Hardness of LWE

$a_i \leftarrow \mathbb{Z}_q^n \qquad b_i = \langle s, a_i \rangle + e_i \in \mathbb{Z}_q$

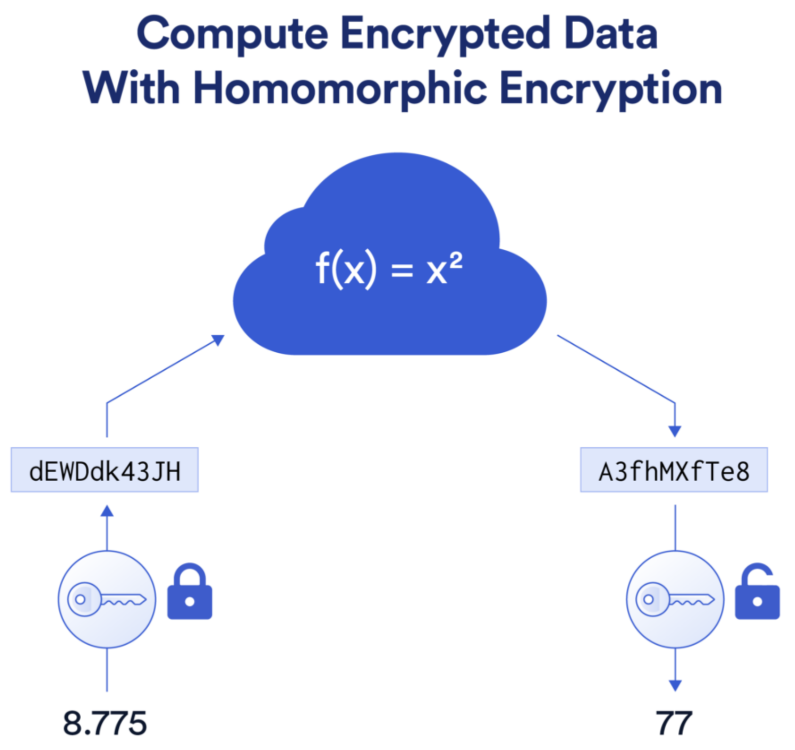
$e_i \leftarrow \chi$ (Discrete Gaussian with variance $\alpha q/\sqrt{2\pi}$)

- From (worst-case) lattice problems.
- For $\alpha q > 2\sqrt{n}, q = poly(n)$

  Regev [Reg05]: quantum reduction from two lattice problems
- Classical reductions:
  - Peikert [Pei09]: classical reduction from a lattice problem for exponential q
  - [BLPRS13]: Equivalent hardness of LWE keeping $n \log_2 q$ fixed.

Versatility of LWE

- Public Key Encryption
- Advanced Primitives
  - Fully Homomorphic Encryption (FHE)
  - Attribute Based Encryption (ABE)
  - Indistinguishability Obfuscation (iO)
  - Lossy Trapdoor Functions (LTDF)
  - Certifiable Deletion
  - Quantum Homomorphic Encryption



Some useful Math and Quantum

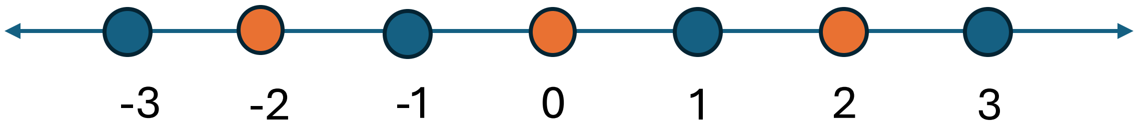
- Notations
  - $\omega_q := \exp(2\pi\iota/q);\ \rho_r(x) = \exp(-\pi x^2/r^2)$
- Discrete Fourier Transform
  - For $f: \mathbb{Z}_q \to \mathbb{C}$, its discrete fourier transform: $\hat{f}(x) = \sum_{y\in\mathbb{Z}_q} \omega_q^{xy} f(y)$
- Quantum Fourier Transform
  - QFT_q: A quantum gate; $\sum_{x\in\mathbb{Z}_q} f(x)|x\rangle \xrightarrow{QFT_q} \sum_{y\in\mathbb{Z}_q} \hat{f}(y)|y\rangle$
  - Efficient to implement: uses $poly \log q$ gates
- Poisson Summation Formula
  - $\rho(\mathbb{Z}+u) = r\sum_{x\in\mathbb{Z}} \exp(2\pi\iota x u)\, \rho_{1/r}(x)$
- Gaussian state preparation
  - We can efficiently prepare a state close to $\sum_{x\in\mathbb{Z}} \rho_r(x)|x\rangle$

Hidden Subgroup Problem

Given:

- A group G (its generators)
- $f: G \to COLORS$
  - $f(g_1) = f(g_2)$ iff $g_1 H = g_2 H$
  - Given as an oracle

Let $H \leq G$



Task: Find H (its generators)

- If G is finite and abelian, we have efficient quantum algorithms.

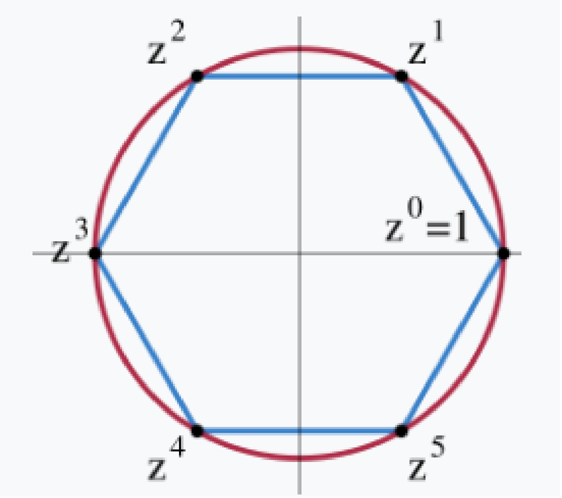
Problem	**Group (G)**	**Hidden Subgroup (H)**
Deutsch-Jozsa	$\mathbb{Z}_2^n$	$H = \mathbb{Z}_2^n$ (Constant) or $H = \{0\}$ (Balanced)
Simon's Problem	$\mathbb{Z}_2^n$	$H = \{0, s\}$ for a secret string s
Period Finding	$\mathbb{Z}$	$H = r\mathbb{Z}$ (Multiples of order r)

Dihedral Hidden Subgroup Problem

Dihedral Group of order $2q$: $D_q := \langle r, t \mid r^2 = t^q = 1,\ rtr = t^{-1} \rangle$

$$\cong \mathbb{Z}_2 \ltimes \mathbb{Z}_q$$

$$(a,x)\cdot(b,y) := (a+b, x+(-1)^a y)$$



Hidden Subgroup: $\mathrm{H} = \{(0,0),(1,s)\}$ for $s \in \mathbb{Z}_q$

Oracle: $f: G \to COLORS$; $f(g_1) = f(g_2)$ iff $g_1 H = g_2 H$

$(0,z)\cdot H = \{(0,z),(1,z+s)\}$

$(1,z)\cdot H = \{(1,z),(0,z-s)\}$ $\quad \therefore f\big((0,z)\big) = f\big((1,z+s)\big)\ \forall z \in \mathbb{Z}_q$

A preprocessing : Get a superposition state of a coset

$$\sum_{x\in\mathbb{Z}_q, a\in\mathbb{Z}_2} |a,x\rangle\,|0\rangle \xrightarrow{\text{Oracle } f} \sum_{x\in\mathbb{Z}_q, a\in\mathbb{Z}_2} |a,x\rangle\,|f((a,x))\rangle \xrightarrow{\text{Measure last register}} |0,z\rangle + |1,z+s\rangle$$

(Unif. rand. $z \in \mathbb{Z}_q$)

Dihedral Coset states

Hidden Subgroup: $H = \{(0,0), (1,s)\}$ for $s \in \mathbb{Z}_q$

We can create random Dihedral Coset states: $|0,z\rangle + |1,z+s\rangle$

Now we'll apply QFT on first register

$$|0,z\rangle + |1,z+s\rangle \xrightarrow{QFT \text{ on } 2^{\text{nd}} \text{ register}} \sum_{k\in\mathbb{Z}_q} \left(\omega_q^{kz}|0,k\rangle + \omega_q^{k(z+s)}|1,k\rangle\right)$$

(Unif. rand. in $\mathbb{Z}_q$)

$$\xrightarrow{\text{Measure } 2^{\text{nd}} \text{ register}} k,\ |\psi_k\rangle := |0\rangle + \omega_q^{ks}|1\rangle$$

If we had $|\psi_{q/2}\rangle = |0\rangle + (-1)^s|1\rangle \xrightarrow{\text{Measure in } |\pm\rangle \text{ basis}}$ Get last bit of s

Kuperberg's idea: Collect lots of $\{k,\ |\psi_k\rangle\}$ and combine them cleverly to get $|\psi_{q/2}\rangle$

Combining: $|\psi_k\rangle|\psi_{k'}\rangle \xrightarrow{CNOT} |\psi_{k+k'}\rangle|0\rangle + \omega_q^{sk'}|\psi_{k-k'}\rangle|1\rangle$

Given $\exp\left(\Theta\left(\sqrt{\log q}\right)\right)$ samples, can find s in $\exp\left(\Theta\left(\sqrt{\log q}\right)\right)$ time

LWE reduces to (faulty) DCP

Let's work with 1-dimensional LWE.

LWE input: $\boldsymbol{a} \leftarrow \mathbb{Z}_q^{m\times 1}, \boldsymbol{b} = s\boldsymbol{a} + \boldsymbol{e}$

Secret $s \in \mathbb{Z}_q$ $e \leftarrow$ Discrete Gaussian of width αq

Partition $\mathbb{Z}_q^m$ into hypercubes of side length w

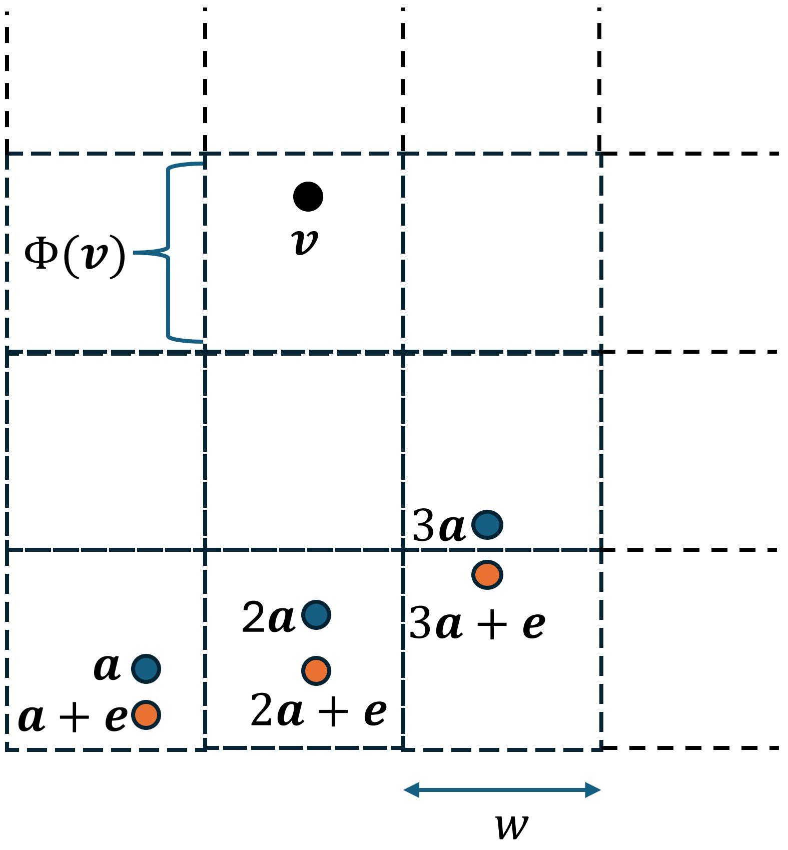
$\Phi(\boldsymbol{v})$: hypercube corresponding to $\boldsymbol{v} \in \mathbb{Z}_q^m$

Choose w so that

- $\Phi(t\boldsymbol{a} + q\boldsymbol{v}) \neq \Phi(t'\boldsymbol{a} + q\boldsymbol{w})$ for any distinct $t, t' \in \mathbb{Z}_q, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{Z}^m$
- $\Phi(t\boldsymbol{a}) = \Phi(t\boldsymbol{a} + \boldsymbol{e})$ for any t w.h.p.

$w\sqrt{m} \leq O(q)$ $w \gg \alpha q\sqrt{m}$

Recall [BLPRS13]: Equivalent hardness of LWE keeping $n \log_2 q$ fixed.



LWE reduces to (faulty) DCP

RHS of LWE: $\boldsymbol{b} = s\boldsymbol{a} + \boldsymbol{e}$

$\Phi(\boldsymbol{v})$: hypercube corresponding to $\boldsymbol{v} \in \mathbb{Z}_q^m$

Prepare the following state:

$$|0\rangle \sum_{t \in \mathbb{Z}_q} |t\rangle\, |\Phi(t\boldsymbol{a})\rangle + |1\rangle \sum_{t \in \mathbb{Z}_q} |t\rangle\, |\Phi(\boldsymbol{b} + t\boldsymbol{a})\rangle$$

$$= |0\rangle \sum_{t \in \mathbb{Z}_q} |t\rangle\, |\Phi(t\boldsymbol{a})\rangle + |1\rangle \sum_{t' \in \mathbb{Z}_q} |t' - s\rangle\, |\Phi(\boldsymbol{e} + t'\boldsymbol{a})\rangle$$

Measure the last register

Good Case: Both $t\boldsymbol{a}$ and $\boldsymbol{e} + t\boldsymbol{a}$ belong to the same cell

We are left with $|0, t\rangle + |1, t - s\rangle$ This is a Dihedral coset state!

Bad Case: $t\boldsymbol{a}$ and $\boldsymbol{e} + t\boldsymbol{a}$ belong to different cells

We are left with $|b\rangle|t\rangle$ For $b \leftarrow \{0,1\}, t \leftarrow \mathbb{Z}_q$

Probability of bad state: inverse poly in $\log q$

Problem: We can't detect which is the case, so can't throw away a bad state

∴ Can only produce poly many correct states w.h.p. instead of $\exp\left(\Theta\left(\sqrt{\log q}\right)\right)$

LWE ≡ Extrapolated DCP

DCP states: $|0, x_k\rangle + |1, x_k + s\rangle$ For a secret $s \in \mathbb{Z}_q$

Extrapolated DCP states: $\sum_{j \in \mathbb{Z}} f(j)|j, \boldsymbol{x}_k + j \cdot \boldsymbol{s}\rangle$ For some $f: \mathbb{Z} \to \mathbb{C}$

Gaussian EDCP: f is a discrete Gaussian $f(j) = \rho_r(j) = e^{-\pi j^2/r^2}$

[BKSW18]: Quantum equivalence of LWE and Gaussian EDCP

LWE → G-EDCP: Similar idea as LWE → DCP

This time start with $\sum_{j \in \mathbb{Z}_q} \rho_r(j)|j\rangle \sum_{t' \in \mathbb{Z}_q} |t' - js\rangle\, |\Phi(j\boldsymbol{e} + t'\boldsymbol{a})\rangle$ and again measure last register

Good Case: For sufficiently large j, all $j\boldsymbol{e} + t'\boldsymbol{a}$ belong to the same cell

Again, can only produce poly many correct states w.h.p.

LWE ≡ Extrapolated DCP

$\rho_r(j) = e^{-\pi j^2/r^2}$

G-EDCP → LWE:

Want to utilize the Gaussian amplitudes to get LWE samples

Given a G-EDCP state: $\sum_{j \in \mathbb{Z}_q} \rho_r(j) |j\rangle |\boldsymbol{x} + j \cdot \boldsymbol{s} \bmod q\rangle$

$\xrightarrow{\text{QFT on 2}^{\text{nd}}\text{ register}}$ $\sum_{\boldsymbol{a} \in \mathbb{Z}_q^n} \sum_{j \in \mathbb{Z}_q} \omega_q^{\langle \boldsymbol{a}, (\boldsymbol{x} + j \cdot \boldsymbol{s}) \rangle} \rho_r(j) |j\rangle |\boldsymbol{a}\rangle$

$\xrightarrow{\text{Measure 2}^{\text{nd}}\text{ register}}$ $\boldsymbol{a_k}, \sum_{j \in \mathbb{Z}_q} \omega_q^{\langle \boldsymbol{a_k}, (j \cdot \boldsymbol{s}) \rangle} \rho_r(j) |j\rangle$

LHS of LWE sample

LWE ≡ Extrapolated DCP

Poisson Summation:

$$\rho(\mathbb{Z}+u) = r \sum_{x\in\mathbb{Z}} \exp(2\pi\imath xu)\, \rho_{1/r}(x)$$

$$\boldsymbol{a}_k\,, \sum_{j\in\mathbb{Z}_q} \omega_q^{\langle \boldsymbol{a}_k, (j\cdot \boldsymbol{s})\rangle} \rho_r(j)|j\rangle$$

QFT on 1st register $\longrightarrow$

$$\boldsymbol{a}_k\,, \sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \omega_q^{j(\langle \boldsymbol{a}_k, \boldsymbol{s}\rangle + b)} \rho_r(j)|b\rangle$$

Like RHS of LWE sample

Poisson Summation

$$= \boldsymbol{a}_k\,, \sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}} \rho_{1/r}\left(j + \frac{\langle \boldsymbol{a}_k, \boldsymbol{s}\rangle + b}{q}\right)|b\rangle$$

$e := qj + \langle \boldsymbol{a}_k, \boldsymbol{s}\rangle + b$

$$= \boldsymbol{a}_k\,, \sum_{e\in\mathbb{Z}} \rho_{1/r}\left(\frac{e}{q}\right)|\langle -\boldsymbol{a}_k, \boldsymbol{s}\rangle + e \bmod q\rangle$$

Measure $\longrightarrow$

$$\boldsymbol{a}_k\,, \langle -\boldsymbol{a}_k, \boldsymbol{s}\rangle + e_k \bmod q$$

$$\mathbb{P}[e_k] = \rho_{1/r}^2\left(\frac{e_k}{q}\right) = \rho_{\frac{q}{r\sqrt{2}}}(e_k)$$

S|LWE⟩

Another attempt at quantum algorithms for LWE

Chen, Liu and Zhandry [CLZ22] defined quantum versions of LWE.

- $S|LWE\rangle$: Instead of $b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e$, give a quantum state
  - Samples: $\boldsymbol{a} \leftarrow \mathbb{Z}_q^n,\ |\phi\rangle \coloneqq \sum_{e \in \mathbb{Z}_q} f(e) |\langle \boldsymbol{a}, \boldsymbol{s} \rangle + e \bmod q\rangle$
  - Find $\boldsymbol{s}$

If f is discrete Gaussian $f(e) = \rho_r(e)$

Can measure $|\phi\rangle$ to get $\langle \boldsymbol{a}, \boldsymbol{s} \rangle + e \bmod q$ with probability $|f(e)|^2$ (LWE sample)

[CHLLT25] reduce <u>one such sample</u> to a DCP state with inverse subexp probability!

Can start with subexp samples and get subexp DCP states.

Then apply Kuperberg's sieve for a subexp algorithm.

LWE reduces to S|LWE⟩$^{\text{phase}}$

S|LWE⟩$^{\text{phase}}$: Have an unknown phase term in the quantum state

Samples: $\boldsymbol{a} \leftarrow \mathbb{Z}_q^n$, $\boldsymbol{y} \leftarrow D_\theta$, $|\phi\rangle := \sum_{e\in\mathbb{Z}_q} f(e) \cdot \exp\big(2\pi\iota e\theta(y)\big) \cdot |\langle \boldsymbol{a}, \boldsymbol{s}\rangle + e \bmod q\rangle$

Possibly uncomputable function

The unknown phase

A distribution over domain of θ

LWE → G-EDCP with unknown shift → S|LWE⟩$^{\text{phase}}$

$$\sum_{j\in\mathbb{Z}_q} \rho_r(j-c)|j\rangle|\boldsymbol{x}_k + j\cdot \boldsymbol{s} \bmod q\rangle$$

Loosely similar to LWE → G-EDCP

Similar to G-EDCP → LWE

Error prob.: inverse exp instead of inverse poly

Cost: Unknown center c

Couple of open questions

- The unknown phase is small and follows Gaussian distribution, so can making a guess of the phase help?

- Can we reduce more structured variants of LWE to $S|LWE\rangle$ / DCP?
  - Ring-LWE, Module-LWE
    - Instead of vectors, have polynomials (RLWE)/ module over polynomials (MLWE)
    - Advantage: Efficient schemes
    - Used in practical schemes (Kyber, Dilithium)
  - Sparse LWE
    - Each a_i has only $k(\ll n)$ non-zero entries.
    - Motivation: Efficient schemes

Thank You