CS 258: Quantum Cryptography

Mark Zhandry

Previously…

Short Integer Solution (SIS)

Input: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ (short, wide)

Chosen uniformly at random

Goal: find vector $\mathbf{x} \in \mathbb{Z}^m$ such that:

$$\mathbf{A} \cdot \mathbf{x} \bmod q = 0$$

$$0 < |\mathbf{x}| \leq \beta$$

Search LWE

Input: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ (short, wide) Chosen uniformly at random

$\mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q$ where

$\mathbf{s}$ uniform in $\mathbb{Z}_q^n$

$\mathbf{e} \leftarrow D_\sigma^m$

Output: $\mathbf{s}$ (in this regime, $\mathbf{s}$ is whp unique)

Thm (restated)**:** If SIS cannot be solved in quantum polynomial time for $\beta = mq/2\sigma$, then neither can decision LWE with error σ

Now used to justify hardness of LWE

Even earlier…

Group Action

An (abelian) group action is a triple $(\mathbb{G}, \mathcal{X}, *)$ where:

- $\mathbb{G}$ is an (abelian) group, written additively
- $\mathcal{X}$ is a set
- $* : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$ is an efficient binary operation satisfying

$$g * (h * x) = (g + h) * x$$

- There is some element $x_0 \in \mathcal{X}$ that can be efficiently computed
- Usually ask that for each $x, y \in \mathcal{X}$, there exists a unique $g \in \mathbb{G}$ such that $y = g * x$
- Also usually ask that it is possible to efficiently identify elements of $\mathcal{X}$

Thm [Kuperberg]: Dlog in (abelian) group actions can be solved in time $2^{O(\sqrt{\log q})}$, where q is the group order

Broader Picture: Hidden Shifts

Kuperberg actually solves a much more general problem called hidden shift

Given $f_0, f_1 : \mathbb{G} \to \mathcal{X}$ injective, such that $f_1(g) = f_0(a+g)$, find a

($\mathbb{G}$ written additively)

Group action Dlog is a special case of hidden shift where

$$f_0(g) = g * x_0 \qquad f_1(g) = g * x_1 = (g+a) * x_0$$

Today: More Quantum Algorithms for Lattices

LWE as Hidden Shift

Suppose for the moment that LWE had no error

Input: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ (short, wide) Chosen uniformly at random

$\mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} \bmod q$ where

$\mathbf{s}$ uniform in $\mathbb{Z}_q^n$

Output: $\mathbf{s}$ (in this regime, $\mathbf{s}$ is whp unique)

Of course, this is easy due by Gaussian elimination

LWE as Hidden Shift

$$f_0(\mathbf{r}) = \mathbf{A}^T \cdot \mathbf{r} \bmod q$$

$$f_1(\mathbf{r}) = \mathbf{A}^T \cdot \mathbf{r} + \mathbf{u} \bmod q = \mathbf{A}^T \cdot (\mathbf{r} + \mathbf{s}) \bmod q = f_0(\mathbf{r} + \mathbf{s} \bmod q)$$

So solving hidden shift allows us to recover $\mathbf{s}$

Ok, but what about the error $\mathbf{e}$?

Solution: round

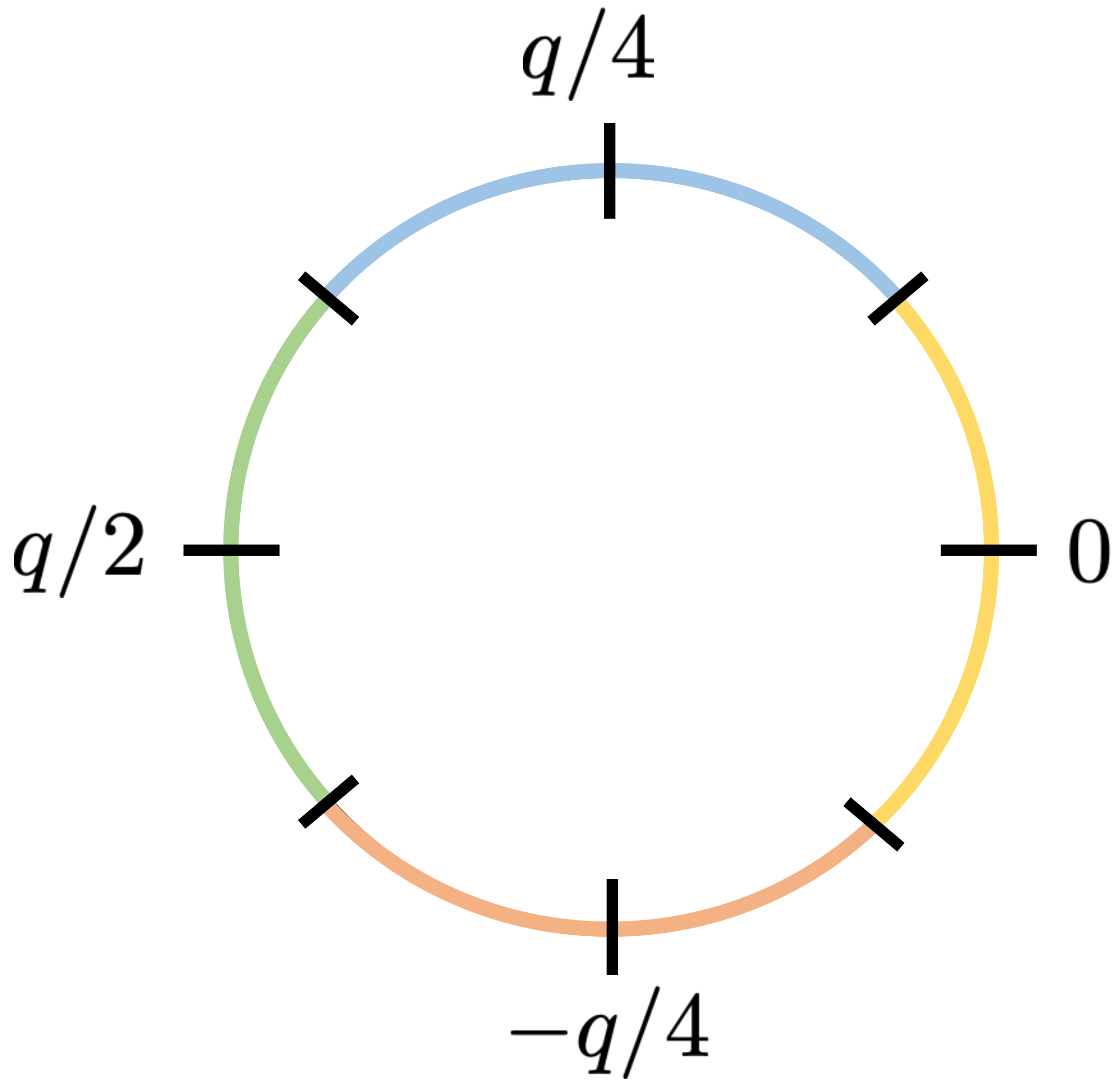
Output closest of $-q/4, 0, q/4, q/2$

$$f_0(\mathbf{r}) = \lfloor \mathbf{A}^T \cdot \mathbf{r} \bmod q \rceil_{q/4}$$

$$f_1(\mathbf{r}) = \lfloor \mathbf{A}^T \cdot \mathbf{r} + \mathbf{u} \bmod q \rceil_{q/4}$$

Idea: if error small enough, rounding eliminates error

$\lfloor x + e \rceil_{q/2} = \lfloor x \rceil_{q/2}$ typically if e small


$q/4$
$q/2$
0
$-q/4$

Now if $\mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q$

$$\begin{aligned} f_1(\mathbf{r}) &= \lfloor \mathbf{A}^T \cdot \mathbf{r} + \mathbf{u} \bmod q \rceil_{q/4} \\ &= \lfloor \mathbf{A}^T \cdot (\mathbf{r} + \mathbf{s}) + \mathbf{e} \bmod q \rceil_{q/4} \\ &=? \lfloor \mathbf{A}^T \cdot (\mathbf{r} + \mathbf{s}) \bmod q \rceil_{q/4} \\ &= f_0(\mathbf{r}) \end{aligned}$$

Need to show:

- Rounding actually gets rid of $\mathbf{e}$
- f_0, f_1 are injective

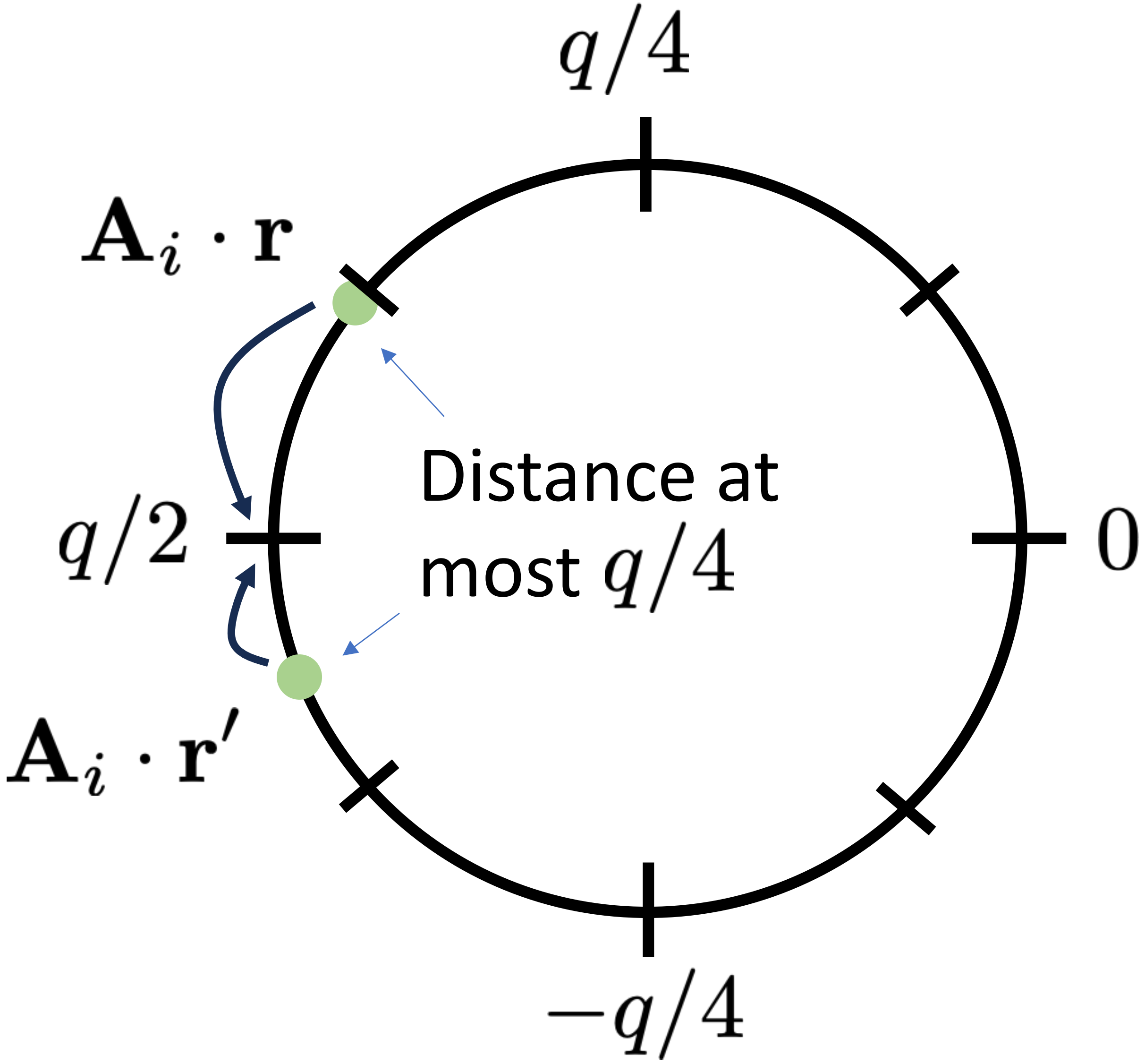
Injectivity

Suffices to only look at f_0 , as hidden shift property will imply injectivity for f_1

$$f_0(\mathbf{r}) = f_0(\mathbf{r}') \iff \lfloor \mathbf{A}^T \cdot \mathbf{r} \bmod q \rceil_{q/4} = \lfloor \mathbf{A}^T \cdot \mathbf{r}' \bmod q \rceil_{q/4}$$
$$\implies |\mathbf{A}^{\mathbf{T}} \cdot (\mathbf{r} - \mathbf{r}')|_\infty \leq q/4$$

Max of absolute values of entries

Injectivity



Injectivity

$$f_0(\mathbf{r}) = f_0(\mathbf{r}') \, , \, \mathbf{r} \neq \mathbf{r}'$$

$$\Rightarrow \exists \mathbf{v} : |\mathbf{A}^T \cdot \mathbf{v} \bmod q|_\infty \leq q/4$$

Claim: with overwhelming probability over $\mathbf{A}$, no such $\mathbf{v}$

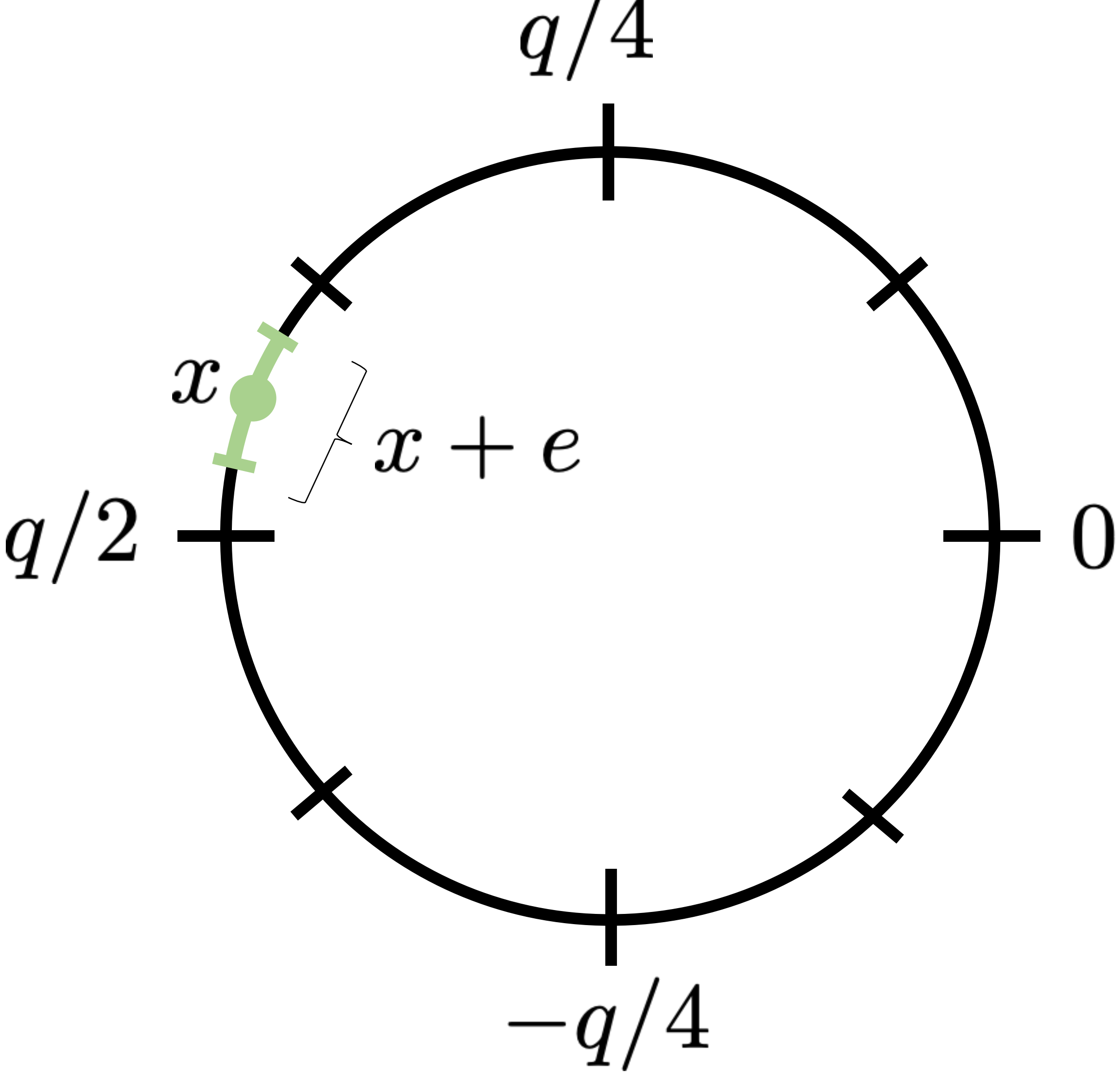
Proof: for any $\mathbf{v}$, $\Pr_{\mathbf{A}_i}[|\mathbf{A}_i \cdot \mathbf{v} \bmod q| \leq q/4] = 1/2$

$$\Rightarrow \Pr_{\mathbf{A}}[|\mathbf{A} \cdot \mathbf{v} \bmod q|_\infty \leq q/4] = 2^{-m} = 2^{-\Omega(n \log q)}$$

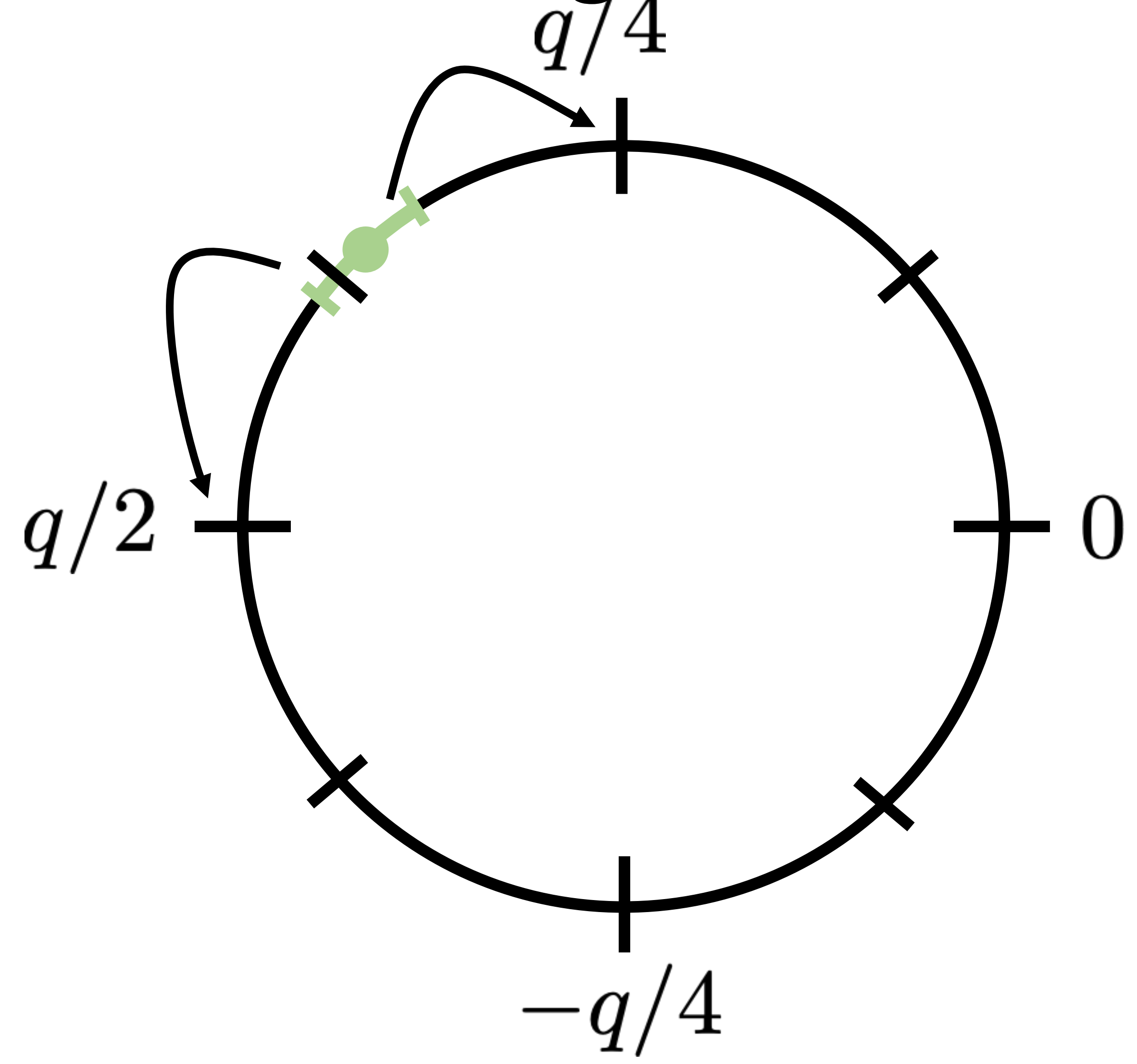
Union-bound over all $2^{n \log q}$ choices of $\mathbf{v}$

$$\Rightarrow \Pr[\exists \mathbf{v} : |\mathbf{A}^T \cdot \mathbf{v} \bmod q|_\infty \leq q/4] \leq 2^{-\Omega(n \log q)}$$

Rounding eliminates $\mathbf{e}$



The problem with rounding



The problem with rounding

Each entry has a $\approx O(\sigma/q)$ chance of being too close to a rounding boundary

Over m entries, probability of some error is $\approx O(\sigma m/q)$

Can we apply Kuperberg?

- Prepare $$\frac{1}{\sqrt{2q^n}} \sum_{\mathbf{r}\in\mathbb{Z}_q^n, b\in\{0,1\}} |\mathbf{r}, b\rangle_{\mathcal{A}} |0\rangle_{\mathcal{B}}$$

- Apply U_f where $f(\mathbf{r}, b) = f_b(\mathbf{r})$:

$$\frac{1}{\sqrt{2q^n}} \sum_{\mathbf{r}\in\mathbb{Z}_q^n, b\in\{0,1\}} |\mathbf{r}, b\rangle_{\mathcal{A}} |f_b(\mathbf{r})\rangle_{\mathcal{B}}$$

$$= \frac{1}{\sqrt{2q^n}} \sum_{\mathbf{r}\in\mathbb{Z}_q^n, b\in\{0,1\}} |\mathbf{r}, b\rangle_{\mathcal{A}} \;\; |\lfloor \mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) + b\mathbf{e} \bmod q\rceil_{q/4}\rangle_{\mathcal{B}}$$

Can we apply Kuperberg?

$$\frac{1}{\sqrt{2q^n}} \sum_{\mathbf{r}\in\mathbb{Z}_q^n, b\in\{0,1\}} |\mathbf{r}, b\rangle_{\mathcal{A}} \; |\lfloor \mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) + b\mathbf{e} \bmod q \rceil_{q/4}\rangle_{\mathcal{B}}$$

- Measure $\mathcal{B}$ → Measurement outcome z
  State collapses to $\mathbf{r}, b$ consistent with z

If $\mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) \bmod q$ is far from rounding boundary,

$$\lfloor \mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) + b\mathbf{e} \bmod q \rceil_{q/4} = \lfloor \mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) \bmod q \rceil_{q/4}$$

➡ State collapses to $\frac{1}{\sqrt{2}}|\mathbf{r}, 0\rangle + \frac{1}{\sqrt{2}}|\mathbf{r} - \mathbf{s} \bmod q, 1\rangle$ ✓

Possible issues with applying Kuperberg

1. The shift lives in $\mathbb{Z}_q^n$ instead of $\mathbb{Z}_{2^n}$

Turns out to not be a problem

2. The errors

Big problem!!!

If $\mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) \bmod q$ is **close** to rounding boundary,

$$\lfloor \mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) + b\mathbf{e} \bmod q \rceil_{q/4} \neq \lfloor \mathbf{A}^T \cdot (\mathbf{r} + b\mathbf{s}) \bmod q \rceil_{q/4}$$

$\Rightarrow$ State collapses to $|\mathbf{r}, b\rangle$

Recall next step of Kuperberg: apply QFT_q to first register, measure

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{t}} |\mathbf{t}, b\rangle e^{i2\pi \mathbf{r}\cdot\mathbf{t}/q} \Rightarrow |\mathbf{t}, b\rangle$$

Combining Samples

Good sample

Bad sample

$$\mathbf{t}_0, |\psi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{-i2\pi\mathbf{s}\cdot\mathbf{t}_0/q}|1\rangle \qquad \mathbf{t}_1, |\psi_1\rangle = |b\rangle$$

$$\mathsf{CNOT}|\psi_0\rangle|\psi_1\rangle = \frac{1}{\sqrt{2}}|0, b\rangle + \frac{1}{\sqrt{2}}e^{-i2\pi\mathbf{s}\cdot\mathbf{t}_0/q}|1, 1-b\rangle$$

Measure second qubit: $|0\rangle$ or $|1\rangle$

Combining with bad samples gives bad samples

Kuperberg requires $2^{O(\sqrt{\log(q^n)})} = 2^{O(\sqrt{n}\log q)}$ samples

If any of those samples are bad, Kuperberg fails

→ Need $\sigma m/q = 2^{-\Omega(\sqrt{n}\log q)}$ to have decent chance of all samples being good

It turns out that, in this regime, classical attacks already exist

Significant open question: can Kuperberg's algorithm be made robust to errors?

A positive solution would give a sub-exponential-time attack on LWE, which would give lattice crypto a significant efficiency penalty

Even beyond LWE, making robust to errors could be important for realizing Kuperberg on a realistic quantum computer

Other possible algorithms

Quasi-polynomial attack on hidden shifts over $\mathbb{Z}_q^n$, when $q = 2^r$

Note that for LWE, hardness is robust to modulus, and can take it to be power of 2

Idea: combine several samples at a time

$$\mathbf{t}_j, |\psi_{\mathbf{t}_j}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{-i2\pi\mathbf{s}\cdot\mathbf{t_j}/q}|1\rangle$$

Write $|\psi_{\mathbf{t}_1}\rangle|\psi_{\mathbf{t}_2}\rangle\cdots$ as

$$\frac{1}{\sqrt{2^\ell}}\sum_{\mathbf{b}\in\{0,1\}^\ell}|\mathbf{b}\rangle e^{-i2\pi\mathbf{s}^T\mathbf{T}\mathbf{b}/q}$$

Where $\mathbf{T} = (\mathbf{t}_1 \;\; \mathbf{t}_2 \;\; \cdots \;\; \mathbf{t}_\ell)$

Idea: combine several samples at a time

$$\frac{1}{\sqrt{2^\ell}} \sum_{\mathbf{b}\in\{0,1\}^\ell} |\mathbf{b}\rangle e^{-i2\pi\mathbf{s}^T\mathbf{T}\mathbf{b}/q}$$

Let's assume mod 2 that $\mathbf{T}$ has a 1-dimensional kernel

Will be true if we choose $\ell \approx n+1$

Idea: combine several samples at a time

$$\frac{1}{\sqrt{2^\ell}} \sum_{\mathbf{b}\in\{0,1\}^\ell} |\mathbf{b}\rangle e^{-i2\pi \mathbf{s}^T \mathbf{T}\mathbf{b}/q}$$

Now apply map $|\mathbf{b}\rangle \mapsto |\mathbf{b}, \mathbf{T}\mathbf{b} \bmod 2\rangle$, and measure second register → $\mathbf{z}$

$$\frac{1}{\sqrt{2}}|\mathbf{b}_0\rangle e^{-i2\pi \mathbf{s}^T \mathbf{T}\mathbf{b}_0/q} + \frac{1}{\sqrt{2}}|\mathbf{b}_1\rangle e^{-i2\pi \mathbf{s}^T \mathbf{T}\mathbf{b}_1/q}$$

$$= e^{-i2\pi \mathbf{s}^T \mathbf{T}\mathbf{b}_0/q} \left(\frac{1}{\sqrt{2}}|\mathbf{b}_0\rangle + \frac{1}{\sqrt{2}}|\mathbf{b}_1\rangle e^{-i2\pi \mathbf{s}^T \mathbf{T}(\mathbf{b}_1 - \mathbf{b}_0)/q} \right)$$

Where $\mathbf{b}_0, \mathbf{b}_1$ are the two values with

$$\mathbf{T}\mathbf{b}_0 \bmod 2 = \mathbf{T}\mathbf{b}_1 \bmod 2 = \mathbf{z}$$

Idea: combine several samples at a time

$$e^{-i2\pi \mathbf{s}^T \mathbf{T}\mathbf{b}_0/q} \left(\frac{1}{\sqrt{2}} |\mathbf{b}_0\rangle + \frac{1}{\sqrt{2}} |\mathbf{b}_1\rangle e^{-i2\pi \mathbf{s}^T \mathbf{T}(\mathbf{b}_1 - \mathbf{b}_0)/q} \right)$$

Now map $|\mathbf{b}_0\rangle \mapsto |0\rangle, |\mathbf{b}_1\rangle \mapsto |1\rangle$

$$e^{-i2\pi \mathbf{s}^T \mathbf{T}\mathbf{b}_0/q} \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle e^{-i2\pi \mathbf{s}^T \mathbf{T}(\mathbf{b}_1 - \mathbf{b}_0)/q} \right)$$

Global phase doesn’t matter: $|\psi_{\mathbf{T}(\mathbf{b}_1 - \mathbf{b}_0)}\rangle$

Idea: combine several samples at a time

Now, observe that $\mathbf{T}(\mathbf{b}_1 - \mathbf{b}_0)$ is even, say $2\mathbf{t}'$

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle e^{-i2\pi \mathbf{s}\cdot 2\mathbf{t}'/q} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle e^{-i2\pi \mathbf{s}\cdot \mathbf{t}'/(q/2)}$$

Reduced the modulus by factor of 2

Each step divides number of samples by $\approx n$

divides modulus by 2

Number of samples needed:

$$\approx n^{\log q} = 2^{(\log n)(\log q)}$$

For LWE parameters, this is $2^{O(\log^2 n)}$, quasi-polynomial!

But, errors still break this algorithm

Multiple shifts

Multiple shifts

$$f_0$$

$$f_1(\mathbf{r}) = f_0(\mathbf{r} + \mathbf{s})$$

$$f_2(\mathbf{r}) = f_0(\mathbf{r} + 2\mathbf{s})$$

...

If we could go all the way to f_q , we'd actually get a periodic function. Maybe something in between makes the problem easier?

Multiple shifts for LWE

$$f_j(\mathbf{r}) = \lfloor \mathbf{A}^T \cdot \mathbf{r} + j\mathbf{u} \bmod q \rceil_{q/4} = \lfloor \mathbf{A}^T \cdot (\mathbf{r} + j\mathbf{s}) + j\mathbf{e} \bmod q \rceil_{q/4}$$

Larger j means larger errors → definitively can't get all the way to periodic

To date, no attack on LWE based on any of these ideas

Next time: when using post-quantum building blocks is not enough