# 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:

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

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

# SIS is a special case of SVP

$$\Lambda_q^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{x} \bmod q = 0\}$$

Full-rank integer lattice

Approximate SVP in $\Lambda_q^{\perp}(\mathbf{A})$ for a random $\mathbf{A}$ is exactly SIS

# The Distribution on e: Discrete Gaussians

$D_\sigma$ = distribution over $\mathbb{Z}$ where

$$\Pr[x \leftarrow D_\sigma] \propto e^{-\pi x^2/\sigma^2}$$

Exact normalization constant is a big infinite sum, but for large $\sigma$ can be approximated as

$$\Pr[x \leftarrow D_\sigma] \approx \frac{1}{\sigma} e^{-\pi x^2/\sigma^2}$$

$D_\sigma^m$ = vector of $m$ iid samples from $D_\sigma$

# 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)

# Decision LWE

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

Case 1: $\mathbf{u} = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q$ where

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

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

Case 2: $\mathbf{u}$ is random

**Output:** guess which case

# LWE is a special case of CVP

$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n \text{ s.t. } \mathbf{x} = \mathbf{A}^T \cdot \mathbf{s} (\bmod q)\}$$

Full-rank integer lattice

LWE = CVP under, for random lattice and random target promised to be close to lattice

# Quantum Algorithms for Lattices

# Recall: The Quantum Fourier Transform (QFT)

$$\mathsf{QFT}_q|x\rangle = \frac{1}{\sqrt{q}}\sum_{y=0}^{q-1} e^{i2\pi xy/q}|y\rangle$$

$$\mathsf{QFT}_q = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots \\ 1 & e^{i2\pi 1/q} & e^{i2\pi 2/q} & e^{i2\pi 3/q} & \cdots \\ 1 & e^{i2\pi 2/q} & e^{i2\pi 4/q} & e^{i2\pi 6/q} & \cdots \\ 1 & e^{i2\pi 3/q} & e^{i2\pi 6/q} & e^{i2\pi 9/q} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

# Convolution Theorem for QFT

Let $|\psi\rangle = \sum_x \alpha_x |x\rangle$ $\qquad$ $|\hat{\psi}\rangle = \mathsf{QFT}_q |\psi\rangle = \sum_y \hat{\alpha}_y |y\rangle$

$|\phi\rangle = \sum_x \beta_x |x\rangle$ $\qquad$ $|\hat{\phi}\rangle = \mathsf{QFT}_q |\phi\rangle = \sum_z \hat{\beta}_z |z\rangle$

$|\tau\rangle = C \sum_x \alpha_x \beta_x |x\rangle$ $\qquad$ What is $|\hat{\tau}\rangle = \mathsf{QFT}_q |\tau\rangle$ ?

# Convolution Theorem for QFT

Let $|\psi\rangle = \sum_x \alpha_x |x\rangle$ $\qquad |\hat{\psi}\rangle = \mathsf{QFT}_q |\psi\rangle = \sum_y \hat{\alpha}_y |y\rangle$

$|\phi\rangle = \sum_x \beta_x |x\rangle$ $\qquad |\hat{\phi}\rangle = \mathsf{QFT}_q |\phi\rangle = \sum_z \hat{\beta}_z |z\rangle$

$$|\tau\rangle = C \sum_x \alpha_x \beta_x |x\rangle$$

**Thm:** $$|\hat{\tau}\rangle = \mathsf{QFT}_q |\tau\rangle = \frac{C}{\sqrt{q}} \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y + z \bmod q\rangle$$

**Thm:** $$|\hat{\tau}\rangle = \mathsf{QFT}_q|\tau\rangle = \frac{C}{\sqrt{q}}\sum_{y,z}\hat{\alpha}_y\hat{\beta}_z|y+z \bmod q\rangle$$

**Proof:**

$$\mathsf{QFT}_q^\dagger\left(\frac{C}{\sqrt{q}}\sum_{y,z}\hat{\alpha}_y\hat{\beta}_z|y+z \bmod q\rangle\right)$$

$$= \frac{C}{q}\sum_{x,y,z}|x\rangle\hat{\alpha}_y\hat{\beta}_z e^{-i2\pi x(y+z)/q}$$

$$= C\sum_x|x\rangle\left(\frac{1}{\sqrt{q}}\sum_y\hat{\alpha}_y e^{-i2\pi xy/q}\right)\left(\frac{1}{\sqrt{q}}\sum_z\hat{\beta}_z e^{-i2\pi xz/q}\right)$$

$$= C\sum_x|x\rangle\alpha_x\beta_x = |\tau\rangle$$

# Quantum Algorithm Blueprint

Goal: find $x$ satisfying two constraints $c_1(x) = c_2(x) = 1$

Each constraint "easy" on its own

Step **n**: Construct $|\tau\rangle = C \sum_x \alpha_x \beta_x |x\rangle$ where:

where $\alpha_x$ has support only on $c_1(x) = 1$

where $\beta_x$ has support only on $c_2(x) = 1$

➡ Overall state has support only on $c_1(x) = c_2(x) = 1$

# Quantum Algorithm Blueprint

Step 1: Construct $|\psi\rangle = \sum_x \alpha_x |x\rangle$ , $|\phi\rangle = \sum_x \beta_x |x\rangle$

Step 2: Construct $|\hat{\psi}\rangle = \mathsf{QFT}_q |\psi\rangle = \sum_y \hat{\alpha}_y |y\rangle$

$$|\hat{\phi}\rangle = \mathsf{QFT}_q |\phi\rangle = \sum_z \hat{\beta}_z |z\rangle$$

$$\Rightarrow |\hat{\psi}\rangle|\hat{\phi}\rangle = \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y, z\rangle$$

# Quantum Algorithm Blueprint

$$|\hat{\psi}\rangle|\hat{\phi}\rangle = \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y, z\rangle$$

vs

$$|\hat{\tau}\rangle = \mathsf{QFT}_q|\tau\rangle = \frac{C}{\sqrt{q}} \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y + z \bmod q\rangle$$

If only we could add in superposition: $|y, z\rangle \mapsto |y + z \bmod q\rangle$

# Quantum Algorithm Blueprint

$$|\hat{\psi}\rangle|\hat{\phi}\rangle = \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y, z\rangle$$

Step 3: Apply controlled add $|y, z\rangle \mapsto |y, y+z \bmod q\rangle$

$$\Rightarrow \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y, y+z \bmod q\rangle$$

Step 4: Somehow "uncompute" $y$ from $y+z \bmod q$

$$\Rightarrow |\hat{\tau}\rangle$$

Step 5: inverse QFT $\Rightarrow |\tau\rangle$

# Attempted Application: SIS
[Regev'05]

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

Set $|\psi\rangle = \frac{1}{q^{(m-n)/2}} \sum_{\mathbf{x}\in\mathbb{Z}_q^m : \mathbf{A}\cdot\mathbf{x} \bmod q = 0} |\mathbf{x}\rangle$

$$|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}^m} \sqrt{\Pr[x \leftarrow D_\gamma]}|\mathbf{x}\rangle$$

Where (say) $\gamma = \beta/m$ so that $|\phi\rangle$ has support only on $|\mathbf{x}| \leq \beta$

# Constructing $|\psi\rangle$

Whp $\mathbf{A}$ will have rank $n$, so kernel will have dimension $m-n$

Let $\mathbf{B} \in \mathbb{Z}_q^{m\times(m-n)}$ be a matrix whose columns span the kernel of $\mathbf{A}$

- Compute $\mathsf{QFT}_q^{\otimes(m-n)}|0\rangle^{\otimes(m-n)} = \frac{1}{q^{(m-n)/2}} \sum_{\mathbf{w}\in\mathbb{Z}_q^{m-n}} |\mathbf{w}\rangle$
- Apply maps $|\mathbf{w}\rangle \mapsto |\mathbf{w}, \mathbf{B}\cdot\mathbf{w} \bmod q\rangle \mapsto |\mathbf{B}\cdot\mathbf{w} \bmod q\rangle$

Can easily compute $\mathbf{w}$ from $\mathbf{B}\cdot\mathbf{w} \bmod q$ ; run in reverse

# Constructing $|\phi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}^m} \sqrt{\Pr[x \leftarrow D_\gamma]}|\mathbf{x}\rangle$

- Let $S$ be somewhat larger than $\gamma$ so that $\Pr_{x\leftarrow D_\gamma}[|x| > S]$ is tiny

- Construct $\frac{1}{\sqrt{2S+1}} \sum_{x=-S}^{S} |x\rangle \left(e^{-\pi x^2/2\gamma^2}|0\rangle + \sqrt{1-e^{-\pi x^2/\gamma^2}}|1\rangle\right)$

- Measure final qubit. If 0, output resulting state. Otherwise, try again

Amplitude on $x$ proportional to $e^{-\pi x^2/2\gamma^2} \propto \sqrt{\Pr[x \leftarrow D_\gamma]}$

- Do the above $m$ times to create $m$ copies of state

# What is $|\hat{\psi}\rangle$ ?

Recall that QFT maps superpositions over group to superposition over quotient group

$$|\hat{\psi}\rangle = \mathsf{QFT}_q^m \frac{1}{q^{(m-n)/2}} \sum_{\mathbf{x}\in\mathbb{Z}_q^m : \mathbf{A}\cdot\mathbf{x} \bmod q = 0} |\mathbf{x}\rangle$$

$$= \frac{1}{q^{n/2}} \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{A}^T \cdot \mathbf{s}\rangle$$

# What is $|\hat{\phi}\rangle$ ?

Intuition from continuous Fourier transform: FT of Gaussian of width $\gamma$ is a Gaussian of width $2\pi/\gamma$

Essentially the same thing happens in the discrete case, with some modifications

# What is $|\hat{\phi}\rangle$ ?

$$|\hat{\phi}\rangle = \mathsf{QFT}_q^m|\phi\rangle = \frac{1}{q^{m/2}}\sum_{\mathbf{e}}|\mathbf{e}\rangle\sum_{\mathbf{x}}\sqrt{\Pr[\mathbf{x}\leftarrow D_\gamma^m]}e^{i2\pi\mathbf{x}\cdot\mathbf{e}/q}$$

$$\approx \frac{1}{(\gamma q)^{m/2}}\sum_{\mathbf{e}}|\mathbf{e}\rangle\sum_{\mathbf{x}}e^{-\pi|\mathbf{x}|^2/2\gamma^2}e^{i2\pi\mathbf{x}\cdot\mathbf{e}/q}$$

$$\approx \frac{1}{(\gamma q)^{m/2}}\sum_{\mathbf{e}}|\mathbf{e}\rangle\int_{\mathbf{x}}e^{-\pi|\mathbf{x}|^2/2\gamma^2}e^{i2\pi\mathbf{x}\cdot\mathbf{e}/q}d\mathbf{x}$$

$$= \left(\frac{2\gamma}{q}\right)\sum_{\mathbf{e}}|\mathbf{e}\rangle e^{-\pi|\mathbf{e}|^2/2(q/2\gamma)^2}$$

$$\approx \sum_{\mathbf{e}}|\mathbf{e}\rangle\sqrt{\Pr[\mathbf{e}\leftarrow D_{q/2\gamma}^m]}$$

Just another discrete Gaussian superposition!

# What is $|\hat{\phi}\rangle$ ?

So the QFT of a discrete Gaussian superposition with width $\gamma$ is (approximately) another discrete Gaussian superposition with width $q/2\gamma$

Note: This derivation assumes $1 \ll \gamma \ll q$

# Quantum Algorithm Blueprint

Step 1: Construct $|\psi\rangle = \sum_x \alpha_x |x\rangle$ , $|\phi\rangle = \sum_x \beta_x |x\rangle$ ✓

Step 2: Construct $|\hat{\psi}\rangle = \mathsf{QFT}_q |\psi\rangle = \sum_y \hat{\alpha}_y |y\rangle$ ✓

$$|\hat{\phi}\rangle = \mathsf{QFT}_q |\phi\rangle = \sum_z \hat{\beta}_z |z\rangle$$

➡ $|\hat{\psi}\rangle|\hat{\phi}\rangle \approx \frac{1}{q^{n/2}} \sum_{s \in \mathbb{Z}_q^n} \sum_{\mathbf{e}} \sqrt{\Pr[\mathbf{e} \leftarrow D_{q/2\gamma}^m]} |\mathbf{A}^T \cdot \mathbf{s} \bmod q, \mathbf{e}\rangle$

# Quantum Algorithm Blueprint

$$|\hat{\psi}\rangle|\hat{\phi}\rangle \approx \frac{1}{q^{n/2}} \sum_{s \in \mathbb{Z}_q^n} \sum_{\mathbf{e}} \sqrt{\Pr[\mathbf{e} \leftarrow D^m_{q/2\gamma}]} |\mathbf{A}^T \cdot \mathbf{s} \bmod q, \mathbf{e}\rangle$$

Step 3: Apply controlled add $|y, z\rangle \mapsto |y, y + z \bmod q\rangle$ ✓

$$\Rightarrow |\hat{\psi}\rangle|\hat{\phi}\rangle \approx \frac{1}{q^{n/2}} \sum_{s \in \mathbb{Z}_q^n} \sum_{\mathbf{e}} \sqrt{\Pr[\mathbf{e} \leftarrow D^m_{q/2\gamma}]} |\mathbf{A}^T \cdot \mathbf{s} \bmod q, \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q\rangle$$

Step 4: Somehow "uncompute" $y$ from $y + z \bmod q$ $\Rightarrow |\hat{\tau}\rangle$

$$y = \mathbf{A}^T \cdot \mathbf{s} \bmod q \qquad y + z \bmod q = \mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q$$

Finding $y$ is equivalent to finding $\mathbf{s}$

Computing $\mathbf{s}$ from $y + z \bmod q$ is *exactly* LWE with error

$$\sigma = q/2\gamma$$

**Thm:** If *decision* LWE with error $\sigma$ can be solved in quantum polynomial-time, then so can SIS with $\beta = mq/2\sigma$

A number of details to make work:

- Get bounds on error of QFT of Discrete Gaussian
- What if search LWE solver only works with non-negligible probability?
- What if only a decisional LWE solver?

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

Now used to justify hardness of LWE

Historical note: we now know that LWE is as hard as SIS via a classical reduction, but this is much more complex and took an extra 5-10 years

There have been a number of attempts to develop quantum algorithms for lattice problems, many following the blueprint using the convolution theorem

Fortunately for post-quantum cryptography, none have worked so far

# Successful uses to QFT + Convolution Theorem

Note: here, $q$ exponential

Yamakawa-Zhandry:

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

Fixed, kernel ≈ low-degree polynomial evaluations

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

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

$$H(x_i) = 1 \forall i$$

Some “random looking” function with one-bit outputs

# Successful uses to QFT + Convolution Theorem

Yamakawa-Zhandry:

**Thm (informal):** If $H$ is modeled as a black box, classical algorithms need exponential-time, but there is a quantum polynomial-time attack

Importance: “random looking” black box functions are exactly how cryptographers often model cryptographic hashing (symmetric key crypto)

Thus, “structure” (e.g. periods, etc) not needed for quantum speedups

# Successful uses to QFT + Convolution Theorem

Note: here, $q$ polynomial

Jordan-Shutty-Wootters-Zalcman-Schmidhuber-King-Isakov-Khattar-Babbush:

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

Fixed, kernel ≈ low-degree polynomial evaluations

$L_1, \cdots, L_m \subseteq \mathbb{Z}_q$

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

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

$x_i \in L_i$ for as many $i$ as possible

Quantum polynomial-time alg satisfying larger fraction of constraints than known classically

# Next time: Lattices vs Group Actions