# OBLIVIOUS LWE SAMPLING IN QUANTUM POLYNOMIAL TIME

Presenter: Pouria Fallahpour [1]

Joint work with Thomas Debris-Alazard [2] and Damien Stehlé [3]

1 ENS Lyon

2 Laboratoire LIX, École Polytechnique

3 ENS Lyon & Cryptolab

# Sampling hard instances of lattices

**Short Integer Solution (SIS)** [Ajtai 96]:

$$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m\times n})$$

Given $\mathbf{A}$, find a short vector $\mathbf{x}$ such that $\mathbf{A}^T\mathbf{x} = \mathbf{0} \mod q$

# Sampling hard instances of lattices

**Short Integer Solution (SIS)** [Ajtai 96]**:**

$$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$$

Given $\mathbf{A}$, find a short vector $\mathbf{x}$ such that $\mathbf{A}^T\mathbf{x} = \mathbf{0} \mod q$

**Learning With Errors (LWE)** [Regev 05]:

$$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n}) \quad \mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^{n}) \qquad \mathbf{e} \sim \chi_\sigma^{\otimes m}$$

Given $\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$, find $(\mathbf{s}, \mathbf{e})$

# Sampling hard instances of lattices

**Short Integer Solution (SIS)** [Ajtai 96]**:**

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$

Given $\mathbf{A}$, find a short vector $\mathbf{x}$ such that $\mathbf{A}^T\mathbf{x} = \mathbf{0} \mod q$

**Learning With Errors (LWE)** [Regev 05]:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$ $\mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^{n})$ $\mathbf{e} \sim \chi_\sigma^{\otimes m}$

Given $\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$, find $(\mathbf{s}, \mathbf{e})$

# What is an aware/oblivious sampler?

SIS:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$

Given $\mathbf{A}$

LWE:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$ $\quad \mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^{n})$ $\quad \mathbf{e} \sim \chi_\sigma^{\otimes m}$

Given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

# What is an aware/oblivious sampler?

SIS:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$

Given $\mathbf{A}$

Don't know the secret

$\Downarrow$

Witness-Obliviousness

LWE:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m \times n})$ $\quad \mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^{n})$ $\quad \mathbf{e} \sim \chi_\sigma^{\otimes m}$

Given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

Planting the secret

$\Downarrow$

Witness-Awareness

# What is an aware/oblivious sampler?

SIS:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m\times n})$

Given $\mathbf{A}$

Don't know the secret

⇓

Witness-Obliviousness

LWE:

$\mathbf{A} \sim \mathcal{U}(\mathbb{Z}_q^{m\times n})$ $\quad \mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^{n})$ $\quad \mathbf{e} \sim \chi_\sigma^{\otimes m}$

Given $\mathbf{A}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

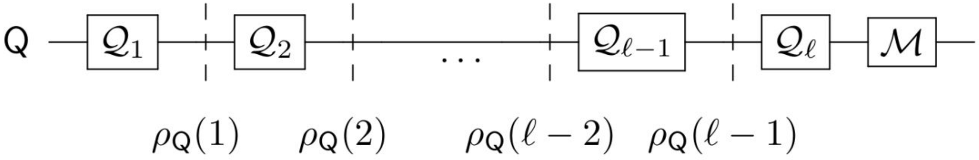
**Lattice Knowledge Assumption**: if $\mathcal{A}$ is an LWE sampler, it is witness-aware.

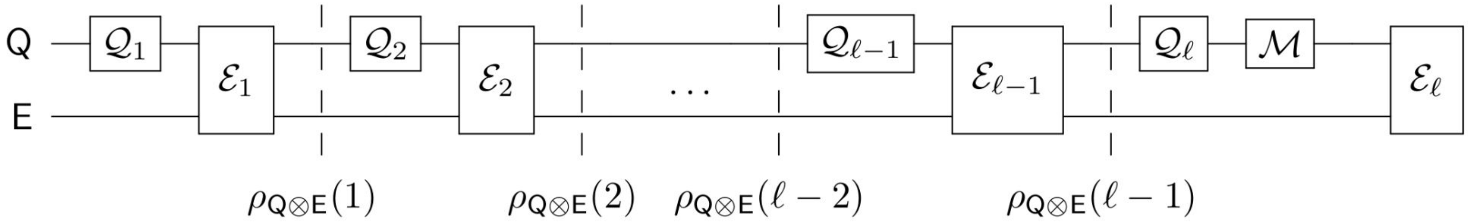
**Our contribution**: A quantum witness-oblivious LWE sampler

Several cryptographic protocols are built based on the lattice knowledge assumption [LMS11,GMNO18,ISW21].

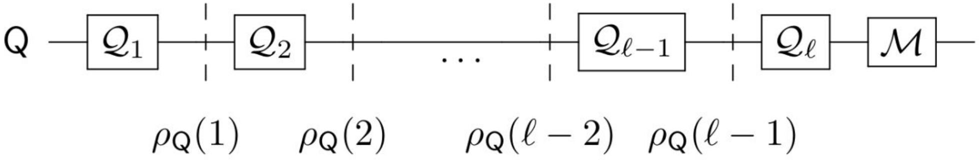
# OBLIVIOUSNESS

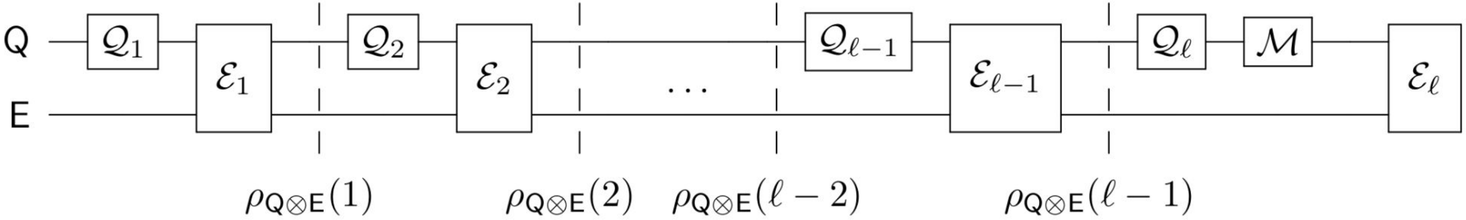
# What is an aware/oblivious sampler?



# What is an aware/oblivious sampler?




For all steps it must hold that: $\mathrm{Tr}_\mathsf{E}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i)) = \rho_\mathsf{Q}(i)$

# THE OBLIVIOUS SAMPLER

# LWE state [Regev 05, SSTX 09]

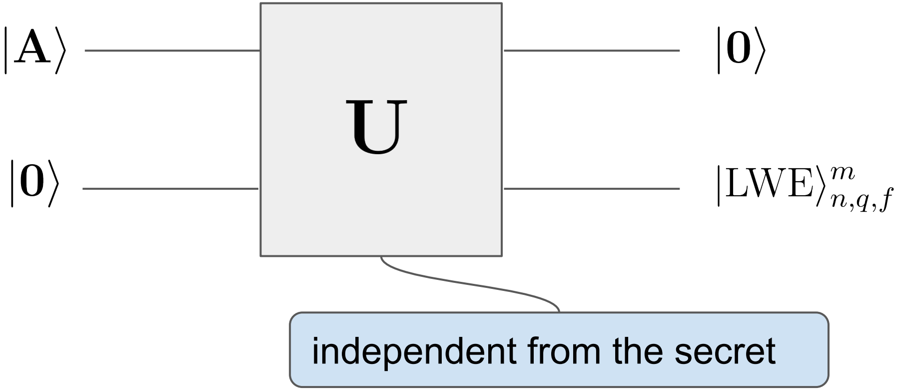
**Idea**: build uniform superposition of LWE samples, then measure

$$|\mathrm{LWE}\rangle_{n,q,f}^{m} \propto \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle \quad \text{with} \quad |f|^2 := (\chi_\sigma)^{\otimes m}$$

# LWE state [Regev 05, SSTX 09]

**Idea**: build uniform superposition of LWE samples, then measure

$$|\mathrm{LWE}\rangle_{n,q,f}^{m} \propto \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle \quad \text{with} \quad |f|^2 := (\chi_\sigma)^{\otimes m}$$



# Building LWE state with [Regev 05, SSTX 09]

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$$

# Building LWE state with [Regev 05, SSTX 09]

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

# Building LWE state with [Regev 05, SSTX 09]

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

Using an LWE solver

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s} - \mathrm{solve}(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e})\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

# Building LWE state with [Regev 05, SSTX 09]

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

Using an LWE solver

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}-\mathrm{solve}(\mathbf{A},\mathbf{A}\mathbf{s}+\mathbf{e})\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{0}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

# Building LWE state with [Regev 05, SSTX 09]

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$$

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

Using an LWE solver

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s} - \mathrm{solve}(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e})\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{0}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

**Not doable in polynomial time**

# TWO INGREDIENTS

# First ingredient: decomposing

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle \qquad\qquad |f|^2 := (\chi_\sigma)^{\otimes m}$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

# First ingredient: decomposing

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle \qquad |f|^2 := (\chi_\sigma)^{\otimes m} = |f_1|^2 \otimes \cdots \otimes |f_m|^2$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

$$= \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f_1(e_1)f_2(e_2)\cdots f_m(e_m)|\mathbf{a}_1^T\mathbf{s}+e_1\rangle \otimes |\mathbf{a}_2^T\mathbf{s}+e_2\rangle \otimes \cdots s \otimes |\mathbf{a}_m^T\mathbf{s}+e_m\rangle$$

# First ingredient: decomposing

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle \qquad |f|^2 := (\chi_\sigma)^{\otimes m} = |f|^2 \otimes \cdots \otimes |f|^2$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

$$= \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(e_1)f(e_2)\cdots f(e_m)|\mathbf{a}_1^T\mathbf{s}+e_1\rangle \otimes |\mathbf{a}_2^T\mathbf{s}+e_2\rangle \otimes \cdots s \otimes |\mathbf{a}_m^T\mathbf{s}+e_m\rangle$$

# First ingredient: decomposing

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle \qquad |f|^2 := (\chi_\sigma)^{\otimes m}$$

$$\longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

$$= \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(e_1)f(e_2)\cdots f(e_m)|\mathbf{a}_1^T\mathbf{s}+e_1\rangle \otimes |\mathbf{a}_2^T\mathbf{s}+e_2\rangle \otimes \cdots s \otimes |\mathbf{a}_m^T\mathbf{s}+e_m\rangle$$

$$= \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$\boxed{|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle}$$

# First ingredient: unambiguous extraction

**Unambiguous Quantum State Discrimination:**

Given $|\psi_j\rangle$ for unknown $j$

Find $j$ without error or return $\perp$ in the case of failure

# First ingredient: unambiguous extraction

**Unambiguous Quantum State Discrimination:**

Given $|\psi_j\rangle$ for unknown $j$

Find $j$ without error or return $\perp$ in the case of failure

$$|\psi_j\rangle := \sum_{e \in \mathbb{Z}_q} f(e)|j+e\rangle \xrightarrow{\text{Optimal POVM [CB98]}} p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

$$\Big\downarrow \text{Optimal POVM}$$

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$\downarrow$$

$$\perp$$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

$$\downarrow \text{Optimal POVM}$$

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$\downarrow$ $\perp$ $\qquad$ $\downarrow$ $\mathbf{a}_2^T\mathbf{s}$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

Optimal POVM $\downarrow$

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$|\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \longrightarrow \perp \qquad |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \longrightarrow \mathbf{a}_2^T\mathbf{s} \qquad |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \longrightarrow \mathbf{a}_{m-1}^T\mathbf{s}$$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

$$\xrightarrow{\text{Optimal POVM}}$$

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$\begin{array}{cccc} \downarrow & \downarrow & \downarrow & \downarrow \\ \perp & \mathbf{a}_2^T\mathbf{s} & \mathbf{a}_{m-1}^T\mathbf{s} & \perp \end{array}$$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

$$\Big\downarrow \text{Optimal POVM}$$

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$\perp \qquad \mathbf{a}_2^T\mathbf{s} \qquad \mathbf{a}_{m-1}^T\mathbf{s} \qquad \perp$$

Apply Gaussian Elimination to recover $\mathbf{s}$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

Optimal POVM

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$\begin{array}{cccc} |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle & |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle & |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle & |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \perp & \mathbf{a}_2^T\mathbf{s} & \mathbf{a}_{m-1}^T\mathbf{s} & \perp \end{array}$$

Apply Gaussian Elimination to recover $\mathbf{s}$

Require $m \gtrsim \dfrac{n}{p_{\mathrm{succ}}} = \dfrac{n}{q} \cdot \dfrac{1}{\min_y |\hat{f}(y)|^2}$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

$$\Big\downarrow \text{ Optimal POVM}$$

$$p_{\mathrm{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

# First ingredient: Gaussian elimination

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes |\psi_{\mathbf{a}_1^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_2^T\mathbf{s}}\rangle \otimes \cdots \otimes |\psi_{\mathbf{a}_{m-1}^T\mathbf{s}}\rangle \otimes |\psi_{\mathbf{a}_m^T\mathbf{s}}\rangle$$

$$\perp \qquad \mathbf{a}_2^T\mathbf{s} \qquad \mathbf{a}_{m-1}^T\mathbf{s} \qquad \perp$$

Apply Gaussian Elimination to recover $\mathbf{s}$

Require $m \gtrsim \dfrac{n}{p_{\text{succ}}} = \dfrac{n}{q} \cdot \dfrac{1}{\min_y |\hat{f}(y)|^2}$

$$|\psi_j\rangle := \sum_{e\in\mathbb{Z}_q} f(e)|j+e\rangle$$

Optimal POVM

$$p_{\text{succ}} = q \cdot \min_y |\hat{f}(y)|^2$$

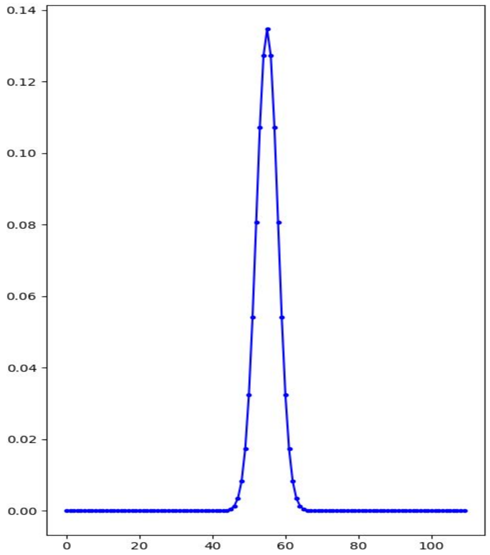
**What we actually do: Naimark's dilation.**

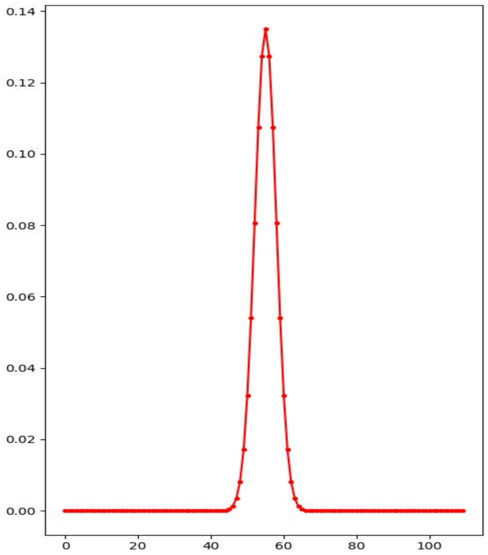
# Summary of the first ingredient

LWE state conditioned on: $m \gtrsim \frac{n}{q} \cdot \frac{1}{\min_y |\hat{f}(y)|^2}$ where $|f|^2 := \chi_\sigma$ (Gaussian)

# Second ingredient: the issue of Gaussian

LWE state conditioned on: $m \gtrapprox n \cdot \mathcal{O}(e^{(q/\sigma)^2})$




Modulus $q$: 110

Standard deviation $\sigma$ : 10.5

Blue: $|f|^2$

Red: $|\hat{f}|^2$

# Second ingredient: adding phases

**idea**: add minus one phases

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\sum_{\mathbf{e}\in\mathbb{Z}_q^m}(-1)^{\theta(\mathbf{e})}f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

# Second ingredient: adding phases

**idea**: add minus one phases

$$\Longrightarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n}\sum_{\mathbf{e}\in\mathbb{Z}_q^m}(-1)^{\theta(\mathbf{e})}f(\mathbf{e})|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

New condition: $m \gtrsim n \cdot \sigma$

# Wrapping up

**Theorem:** We construct a quantum witness-oblivious LWE sampler when the standard deviation is polynomially large.

# Conclusion

- Obliviously sampling instances of LWE
  - New techniques and definitions: robust definition of obliviousness, (-1) phases
  - Maybe a new example of quantum vs classical gap.

- Breaking the security of several proof systems

Thank you!