Lattices: From Worst-Case, to Average-Case, to Cryptography

Chris Peikert
Georgia Institute of Technology

Public Key Cryptography
and the Geometry of Numbers

6 May 2010

Talk Agenda

1. Smoothing and discrete Gaussians
2. From worst-case to average-case
3. Basic crypto applications

Part 1:

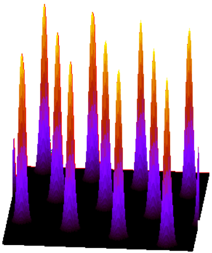
The Smoothing Parameter and Discrete Gaussians

- D. Micciancio, O. Regev (FOCS 2004)
  "Worst-Case to Average-Case Reductions Based on Gaussian Measures"
- C. Gentry, C. Peikert, V. Vaikuntanathan (STOC 2008)
  "Trapdoors for Hard Lattices and New Cryptographic Constructions"

The Smoothing Parameter [AR'04,MR'04]

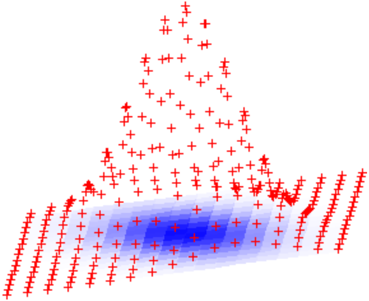
- Gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$. Scaled: $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.

Primal $\mathcal{L}$



$f_s(\mathbf{x}) \propto \rho_s(\mathcal{L} + \mathbf{x})$

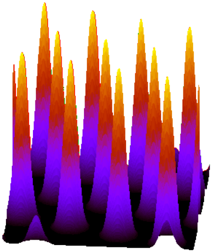
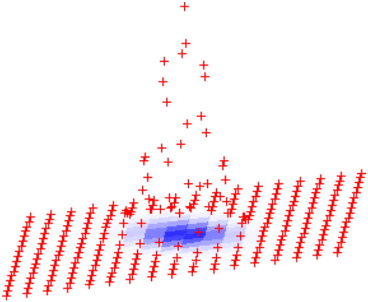
Dual $\mathcal{L}^*$



$\hat{f}(\mathbf{w}) \propto \rho_{1/s}(\mathbf{w})$ for $\mathbf{w} \in \mathcal{L}^*$

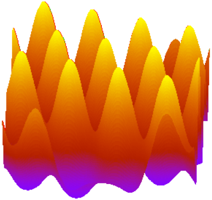
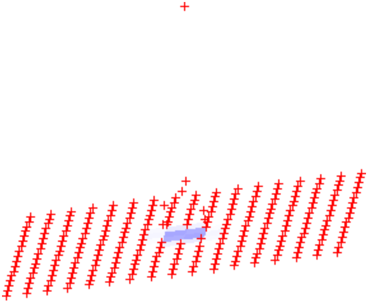
The Smoothing Parameter [AR'04,MR'04]

- Gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$. Scaled: $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.

Primal $\mathcal{L}$	Dual $\mathcal{L}^*$
	
$f_s(\mathbf{x}) \propto \rho_s(\mathcal{L} + \mathbf{x})$	$\hat{f}(\mathbf{w}) \propto \rho_{1/s}(\mathbf{w})$ for $\mathbf{w} \in \mathcal{L}^*$

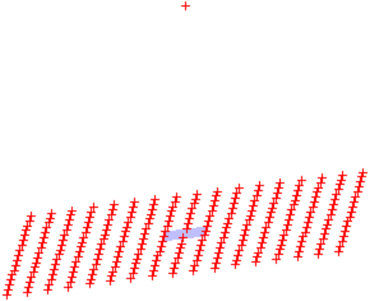
The Smoothing Parameter [AR'04,MR'04]

- Gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$. Scaled: $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.

Primal $\mathcal{L}$	Dual $\mathcal{L}^*$
	
$f_s(\mathbf{x}) \propto \rho_s(\mathcal{L} + \mathbf{x})$	$\hat{f}(\mathbf{w}) \propto \rho_{1/s}(\mathbf{w})$ for $\mathbf{w} \in \mathcal{L}^*$

The Smoothing Parameter [AR'04,MR'04]

- Gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$. Scaled: $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.

Primal $\mathcal{L}$	Dual $\mathcal{L}^*$
	
$f_s(\mathbf{x}) \propto \rho_s(\mathcal{L} + \mathbf{x})$	$\hat{f}(\mathbf{w}) \propto \rho_{1/s}(\mathbf{w})$ for $\mathbf{w} \in \mathcal{L}^*$

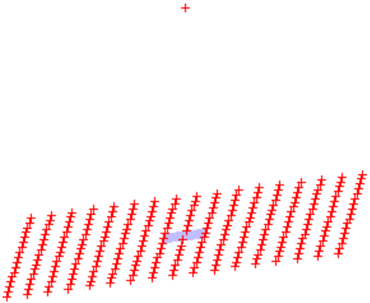
The Smoothing Parameter [AR'04,MR'04]

- Gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$. Scaled: $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.

Primal $\mathcal{L}$

$f_s(\mathbf{x}) \;\propto\; \rho_s(\mathcal{L} + \mathbf{x})$

Dual $\mathcal{L}^*$



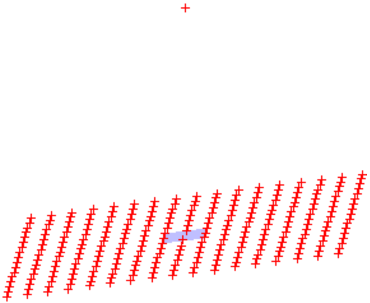
$\hat{f}(\mathbf{w}) \propto \rho_{1/s}(\mathbf{w})$ for $\mathbf{w} \in \mathcal{L}^*$

Definition: Smoothing Parameter

smooth$(\mathcal{L}) = \min s > 0$ such that $\rho(s\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq$ negl(n)

The Smoothing Parameter [AR'04,MR'04]

- Gaussian function $\rho(\mathbf{x}) = e^{-\pi\|\mathbf{x}\|^2}$. Scaled: $\rho_s(\mathbf{x}) = \rho(\mathbf{x}/s)$.

Primal $\mathcal{L}$	Dual $\mathcal{L}^*$
	
$f_s(\mathbf{x}) \;\propto\; \rho_s(\mathcal{L} + \mathbf{x})$	$\hat{f}(\mathbf{w}) \propto \rho_{1/s}(\mathbf{w})$ for $\mathbf{w} \in \mathcal{L}^*$

Key Fact

For $s \geq$ smooth$(\mathcal{L})$, every coset has equal* mass: $\rho_s(\mathcal{L} + \mathbf{x}) \approx \rho_s(\mathcal{L})$.

Smoothing Parameter of $\mathbb{Z}^n$

Theorem

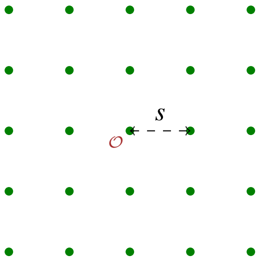
$$\mathsf{smooth}(\mathbb{Z}^n) \leq \omega(\sqrt{\log n})$$

Smoothing Parameter of $\mathbb{Z}^n$

Theorem

$$\text{smooth}(\mathbb{Z}^n) \leq \omega(\sqrt{\log n})$$

Need to show: $\boxed{\rho(s\mathbb{Z}^n \setminus \{\mathbf{0}\}) \leq \text{negl}}$ when $s = \omega(\sqrt{\log n})$.



Smoothing Parameter of $\mathbb{Z}^n$

Theorem

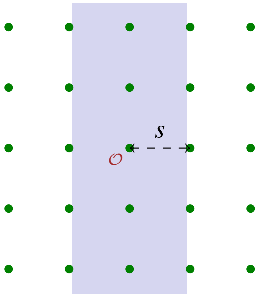
$$\text{smooth}(\mathbb{Z}^n) \leq \omega(\sqrt{\log n})$$

Need to show: $\boxed{\rho(s\mathbb{Z}^n \setminus \{\mathbf{0}\}) \leq \text{negl}}$ when $s = \omega(\sqrt{\log n})$.

Lemma: Tail Bound [Banaszczyk'95]

For *any* lattice $\mathcal{L}$,

$$\rho(\mathcal{L} \setminus \square) \leq 2\exp(-\pi s^2) \cdot \rho(\mathcal{L})$$



Smoothing Parameter of $\mathbb{Z}^n$

Theorem

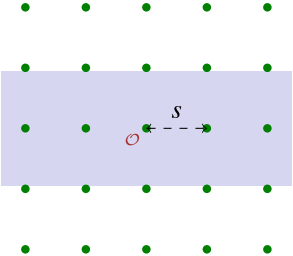
$$\text{smooth}(\mathbb{Z}^n) \le \omega(\sqrt{\log n})$$

Need to show: $\boxed{\rho(s\mathbb{Z}^n \setminus \{\mathbf{0}\}) \le \text{negl}}$ when $s = \omega(\sqrt{\log n})$.

Lemma: Tail Bound **[Banaszczyk'95]**

For *any* lattice $\mathcal{L}$,

$$\rho(\mathcal{L} \setminus \square) \;\le\; 2\exp(-\pi s^2) \cdot \rho(\mathcal{L})$$



Smoothing Parameter of $\mathbb{Z}^n$

Theorem

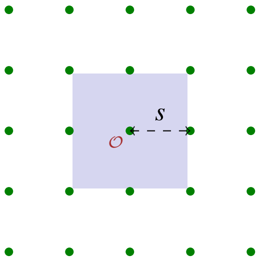
$$\text{smooth}(\mathbb{Z}^n) \leq \omega(\sqrt{\log n})$$

Need to show: $\boxed{\rho(s\mathbb{Z}^n \setminus \{\mathbf{0}\}) \leq \text{negl}}$ when $s = \omega(\sqrt{\log n})$.

Lemma: Tail Bound **[Banaszczyk'95]**

For *any* lattice $\mathcal{L}$,

$$\rho(\mathcal{L} \setminus \blacksquare) \;\leq\; 2\exp(-\pi s^2) \cdot \rho(\mathcal{L})$$



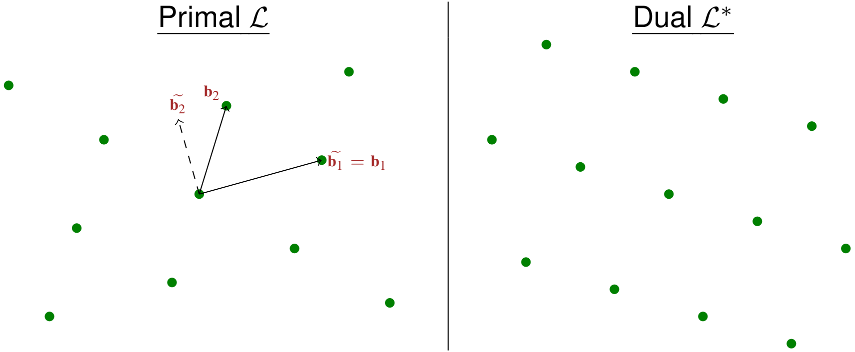
By union bound,

$$\begin{aligned} p := \rho(s\mathbb{Z}^n \setminus \{\mathbf{0}\}) &= \rho(s\mathbb{Z}^n \setminus \blacksquare) \\ &\leq n \cdot \text{negl} \cdot \rho(s\mathbb{Z}^n) \\ &= \text{negl} \cdot (1+p). \qquad \square \end{aligned}$$

Smoothing Parameter of Any Lattice [MR'04,GPV'08]

- Gram-Schmidt orthogonalization $\widetilde{\mathbf{B}}$.

(Note: $\|\widetilde{\mathbf{B}}\| := \max_i \|\widetilde{\mathbf{b}}_i\| \leq \max_i \|\mathbf{b}_i\|$)



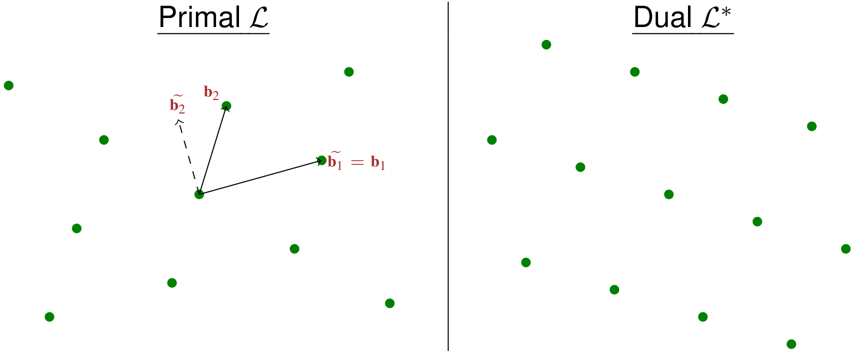
Smoothing Parameter of Any Lattice [MR'04,GPV'08]

- Gram-Schmidt orthogonalization $\widetilde{\mathbf{B}}$.

(Note: $\|\widetilde{\mathbf{B}}\| := \max_i \|\widetilde{\mathbf{b}_i}\| \leq \max_i \|\mathbf{b}_i\|$)

Theorem

Let $\mathbf{B}$ be any basis of $\mathcal{L}$. Then $\text{smooth}(\mathcal{L}) \leq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$.



Smoothing Parameter of Any Lattice [MR'04,GPV'08]

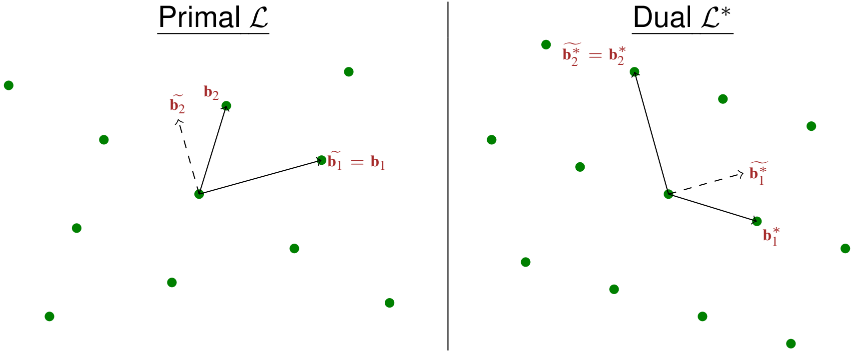
- Gram-Schmidt orthogonalization $\widetilde{\mathbf{B}}$.

(Note: $\|\widetilde{\mathbf{B}}\| := \max_i \|\widetilde{\mathbf{b}_i}\| \leq \max_i \|\mathbf{b}_i\|$)

Theorem

Let $\mathbf{B}$ be any basis of $\mathcal{L}$. Then $\text{smooth}(\mathcal{L}) \leq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$.

- Dual basis: $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = \delta_{ij}$. (GSO in reverse.)



Smoothing Parameter of Any Lattice [MR'04,GPV'08]

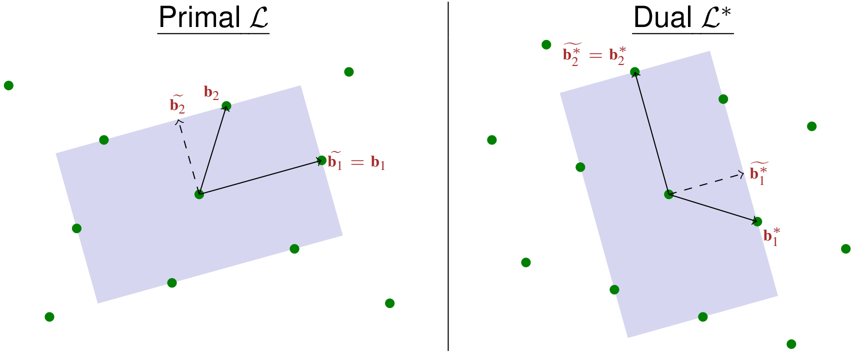
- Gram-Schmidt orthogonalization $\widetilde{\mathbf{B}}$.

(Note: $\|\widetilde{\mathbf{B}}\| := \max_i \|\widetilde{\mathbf{b}}_i\| \leq \max_i \|\mathbf{b}_i\|$)

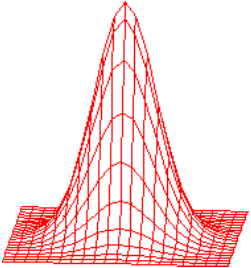
Theorem

Let $\mathbf{B}$ be any basis of $\mathcal{L}$. Then $\text{smooth}(\mathcal{L}) \leq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$.

- Dual basis: $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = \delta_{ij}$. (GSO in reverse.) Fact: $\|\widetilde{\mathbf{b}_i^*}\| = 1/\|\widetilde{\mathbf{b}_i}\|$

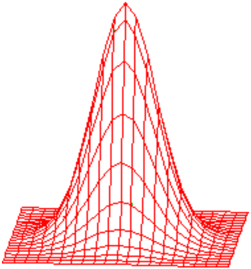


Discrete Gaussians over Lattices



Suppose $\mathbf{x} \sim \text{Gauss}(s)$ for $s \geq \text{smooth}(\mathcal{L})$.

Discrete Gaussians over Lattices

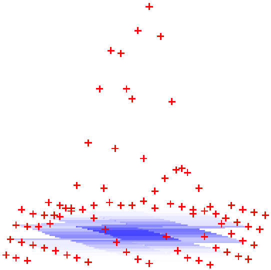


Suppose $\mathbf{x} \sim \text{Gauss}(s)$ for $s \geq \text{smooth}(\mathcal{L})$.

1. $\mathbf{x}$ belongs to uniform* coset $\mathcal{L} + \mathbf{c}$

   $[\forall \mathbf{c},\ \rho_s(\mathcal{L} + \mathbf{c}) \approx \rho_s(\mathcal{L})]$

Discrete Gaussians over Lattices



Suppose $\mathbf{x} \sim \text{Gauss}(s)$ for $s \geq \text{smooth}(\mathcal{L})$.

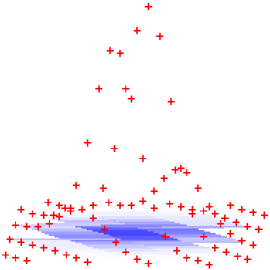
1. $\mathbf{x}$ belongs to uniform* coset $\mathcal{L} + \mathbf{c}$

   $[\forall \mathbf{c},\ \rho_s(\mathcal{L} + \mathbf{c}) \approx \rho_s(\mathcal{L})]$

2. Given $\mathbf{c}$, conditional distrib of $\mathbf{x} \in \mathcal{L} + \mathbf{c}$ is:

$$D_{\mathcal{L}+\mathbf{c},s}(\mathbf{x}) \ \propto \ \rho_s(\mathbf{x}).$$

Discrete Gaussians over Lattices



Suppose $\mathbf{x} \sim \text{Gauss}(s)$ for $s \geq \text{smooth}(\mathcal{L})$.

1. $\mathbf{x}$ belongs to uniform* coset $\mathcal{L} + \mathbf{c}$

   $[\forall \mathbf{c},\ \rho_s(\mathcal{L} + \mathbf{c}) \approx \rho_s(\mathcal{L})]$

2. Given $\mathbf{c}$, conditional distrib of $\mathbf{x} \in \mathcal{L} + \mathbf{c}$ is:

$$D_{\mathcal{L}+\mathbf{c},s}(\mathbf{x}) \ \propto \ \rho_s(\mathbf{x}).$$

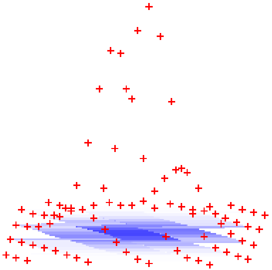
Gaussian-like Properties

1. High probability tail bounds: for $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$,

$$\|\mathbf{x}\| \leq s \cdot \sqrt{n}$$

for unit $\mathbf{u}$, $$|\langle \mathbf{x}, \mathbf{u} \rangle| \leq s \cdot \omega(\sqrt{\log n})$$

Discrete Gaussians over Lattices



Suppose $\mathbf{x} \sim \text{Gauss}(s)$ for $s \geq \text{smooth}(\mathcal{L})$.

1. $\mathbf{x}$ belongs to uniform* coset $\mathcal{L} + \mathbf{c}$

   $[\forall \mathbf{c},\ \rho_s(\mathcal{L} + \mathbf{c}) \approx \rho_s(\mathcal{L})]$

2. Given $\mathbf{c}$, conditional distrib of $\mathbf{x} \in \mathcal{L} + \mathbf{c}$ is:

$$D_{\mathcal{L}+\mathbf{c},s}(\mathbf{x}) \ \propto\ \rho_s(\mathbf{x}).$$

Gaussian-like Properties

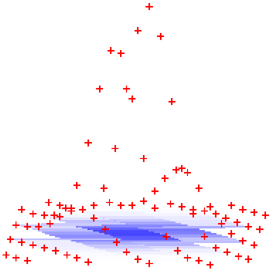
1. High probability tail bounds: for $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$,

$$\|\mathbf{x}\| \leq s \cdot \sqrt{n}$$

$$\text{for unit } \mathbf{u},\quad |\langle \mathbf{x}, \mathbf{u} \rangle| \leq s \cdot \omega(\sqrt{\log n})$$

2. Additive: if $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$ and $\mathbf{y} \sim D_{\mathcal{L}+\mathbf{d},t}$, then $\mathbf{x} + \mathbf{y} \sim D_{\mathcal{L}+\mathbf{c}+\mathbf{d},\sqrt{s^2+t^2}}$

Discrete Gaussians over Lattices



Suppose $\mathbf{x} \sim$ Gauss(s) for $s \geq$ smooth$(\mathcal{L})$.

1. $\mathbf{x}$ belongs to uniform* coset $\mathcal{L} + \mathbf{c}$

   $[\forall \mathbf{c},\ \rho_s(\mathcal{L} + \mathbf{c}) \approx \rho_s(\mathcal{L})]$

2. Given $\mathbf{c}$, conditional distrib of $\mathbf{x} \in \mathcal{L} + \mathbf{c}$ is:

$$D_{\mathcal{L}+\mathbf{c},s}(\mathbf{x}) \ \propto \ \rho_s(\mathbf{x}).$$

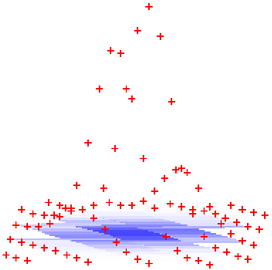
Gaussian-like Properties

1. High probability tail bounds: for $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$,

$$\begin{aligned} \|\mathbf{x}\| &\leq s \cdot \sqrt{n} \\ \text{for unit } \mathbf{u}, \quad |\langle \mathbf{x}, \mathbf{u} \rangle| &\leq s \cdot \omega(\sqrt{\log n}) \end{aligned}$$

2. Additive: if $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$ and $\mathbf{y} \sim D_{\mathcal{L}+\mathbf{d},t}$, then $\mathbf{x} + \mathbf{y} \sim D_{\mathcal{L}+\mathbf{c}+\mathbf{d},\sqrt{s^2+t^2}}$
3. Unpredictable: min-entropy $\geq n$

Discrete Gaussians over Lattices



Suppose $\mathbf{x} \sim \mathsf{Gauss}(s)$ for $s \geq \mathsf{smooth}(\mathcal{L})$.

1. $\mathbf{x}$ belongs to uniform* coset $\mathcal{L} + \mathbf{c}$

   $[\forall \mathbf{c},\ \rho_s(\mathcal{L} + \mathbf{c}) \approx \rho_s(\mathcal{L})]$

2. Given $\mathbf{c}$, conditional distrib of $\mathbf{x} \in \mathcal{L} + \mathbf{c}$ is:

$$D_{\mathcal{L}+\mathbf{c},s}(\mathbf{x}) \ \propto \ \rho_s(\mathbf{x}).$$

Gaussian-like Properties

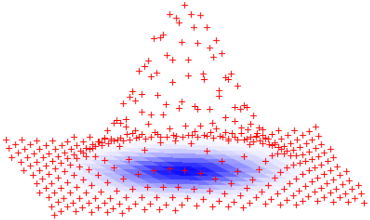
1. High probability tail bounds: for $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$,

$$\begin{aligned} \|\mathbf{x}\| &\leq s \cdot \sqrt{n} \\ \text{for unit } \mathbf{u},\quad |\langle \mathbf{x}, \mathbf{u} \rangle| &\leq s \cdot \omega(\sqrt{\log n}) \end{aligned}$$

2. Additive: if $\mathbf{x} \sim D_{\mathcal{L}+\mathbf{c},s}$ and $\mathbf{y} \sim D_{\mathcal{L}+\mathbf{d},t}$, then $\mathbf{x} + \mathbf{y} \sim D_{\mathcal{L}+\mathbf{c}+\mathbf{d},\sqrt{s^2+t^2}}$
3. Unpredictable: min-entropy $\geq n$
4. Many more ...

Sampling a Discrete Gaussian [GPV'08,P'10]

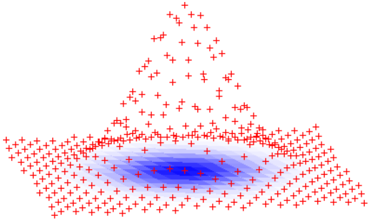
- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, efficiently sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$

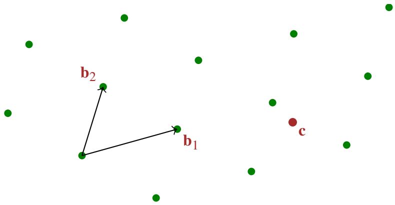


Sampling a Discrete Gaussian [GPV'08,P'10]

- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, <u>efficiently</u> sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$

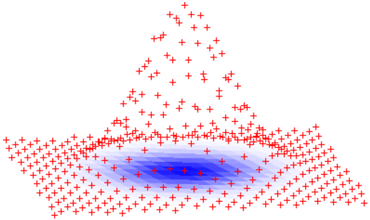
- "Nearest-plane" algorithm w/ randomized rounding [Babai'86,Klein'00]

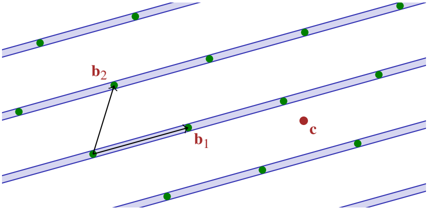




Sampling a Discrete Gaussian [GPV'08,P'10]

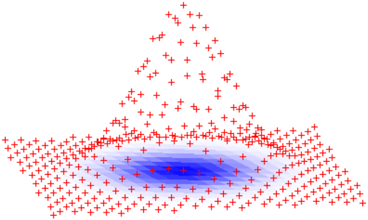
- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, efficiently sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$
- "Nearest-plane" algorithm w/ randomized rounding [Babai'86,Klein'00]

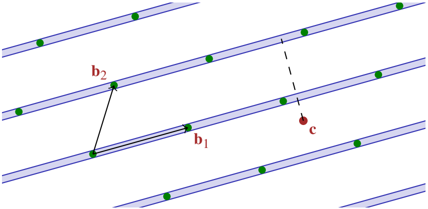




Sampling a Discrete Gaussian [GPV'08,P'10]

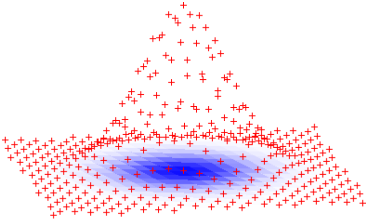
- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, <u>efficiently</u> sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$
- "Nearest-plane" algorithm w/ randomized rounding [Babai'86,Klein'00]

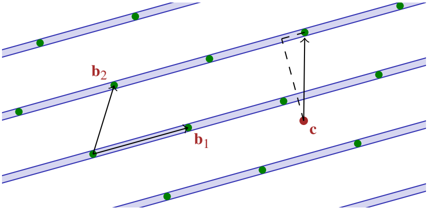




Sampling a Discrete Gaussian [GPV'08,P'10]

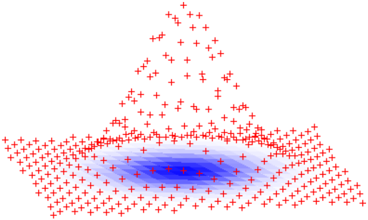
- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, efficiently sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$
- "Nearest-plane" algorithm w/ randomized rounding [Babai'86,Klein'00]

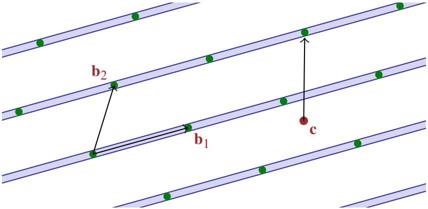




Sampling a Discrete Gaussian [GPV'08,P'10]

- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, <u>efficiently</u> sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$
- "Nearest-plane" algorithm w/ randomized rounding [Babai'86,Klein'00]



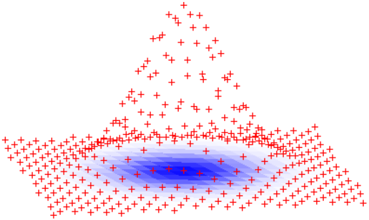


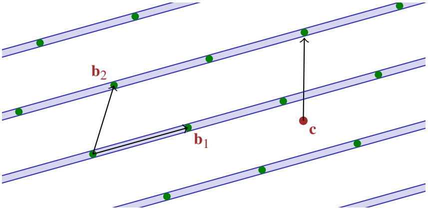
- Proof: by smoothing, $D_{\mathcal{L}-\mathbf{c},s}(\text{plane})$ depends only on $\text{dist}(\mathbf{c}, \text{plane})$

Sampling a Discrete Gaussian [GPV'08,P'10]

- Given basis $\mathbf{B}$ and $\mathbf{c} \in \mathbb{R}^n$, <u>efficiently</u> sample $D_{\mathcal{L}-\mathbf{c},s}$ for $s \geq \|\widetilde{\mathbf{B}}\|$
  - ⋆ Output distribution is 'oblivious' to input basis $\mathbf{B}$

- "Nearest-plane" algorithm w/ randomized rounding [Babai'86,Klein'00]





- Proof: by smoothing, $D_{\mathcal{L}-\mathbf{c},s}$(plane) depends only on $\mathrm{dist}(\mathbf{c}, \text{plane})$

- [P'10]: More efficient, parallel algorithm for $s \geq \sigma_1(\mathbf{B})$ ($\approx \|\widetilde{\mathbf{B}}\|$, often)

Part 2:

From Worst-Case to Average-Case & Basic Crypto Applications

- M. Ajtai (STOC 1996)
  "Generating Hard Instances of Lattice Problems"
- [MR'04, GPV'08]
- O. Regev (STOC 2005)
  "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography"
- C. Peikert (STOC 2009)
  "Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem"

'Short Integer Solution' (SIS) Problem [Ajtai'96]

- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \quad \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} \quad \cdots \quad \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \quad \in \mathbb{Z}_q^n$$

‘Short Integer Solution’ (SIS) Problem [Ajtai’96]

- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$
- Goal: find nontrivial $z_1, \ldots, z_m \in \{0, \pm 1\}$ such that:

$$z_1 \cdot \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + z_2 \cdot \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} + \cdots + z_m \cdot \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{0} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

‘Short Integer Solution’ (SIS) Problem [Ajtai’96]

- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

'Short Integer Solution' (SIS) Problem [Ajtai'96]

- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \\ & & \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

- For $\boxed{m > n \lg q,}$ $\exists\, \mathbf{x} \neq \mathbf{x}' \in \{0, 1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}' \Rightarrow \mathbf{x} - \mathbf{x}'$ is a soln

'Short Integer Solution' (SIS) Problem [Ajtai'96]

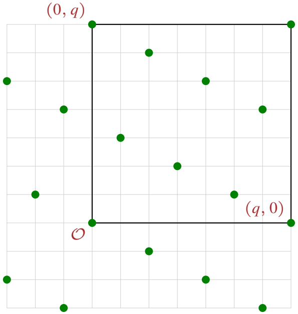
- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \mathbf{z} \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

- For $\boxed{m > n \lg q,}$ $\exists\, \mathbf{x} \neq \mathbf{x}' \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}' \Rightarrow \mathbf{x} - \mathbf{x}'$ is a soln

- Solutions form a 'q-ary' integer lattice:

$$\mathcal{L}^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \;:\; \mathbf{A}\mathbf{z} = \mathbf{0}\} \subseteq \mathbb{Z}^m$$



‘Short Integer Solution’ (SIS) Problem [Ajtai’96]

- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$
- Goal: find nontrivial ‘short’ $\mathbf{z} \in \mathbb{Z}^m$ such that:

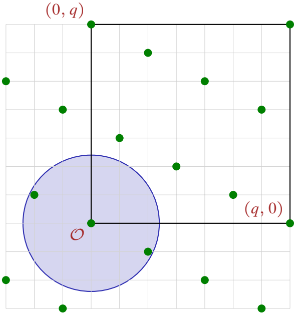
$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \mathbf{z} \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

- For $\boxed{m > n \lg q,}$ $\exists\, \mathbf{x} \neq \mathbf{x}' \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}' \Rightarrow \mathbf{x} - \mathbf{x}'$ is a soln

- Solutions form a ‘q-ary’ integer lattice:

$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \;:\; \mathbf{A}\mathbf{z} = \mathbf{0}\} \subseteq \mathbb{Z}^m$$

- Relaxation: length bound $\beta > \sqrt{n \lg q}$



'Short Integer Solution' (SIS) Problem [Ajtai'96]

- Given: uniform $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$
- Goal: find nontrivial 'short' $\mathbf{z} \in \mathbb{Z}^m$ such that:

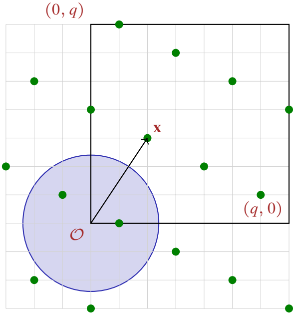
$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \mathbf{z} \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

- For $\boxed{m > n \lg q,}$ $\exists\, \mathbf{x} \neq \mathbf{x}' \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}' \Rightarrow \mathbf{x} - \mathbf{x}'$ is a soln

- Solutions form a 'q-ary' integer lattice:

$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ :\ \mathbf{A}\mathbf{z} = \mathbf{0}\} \subseteq \mathbb{Z}^m$$

- Relaxation: length bound $\beta > \sqrt{n \lg q}$
- Syndrome $\mathbf{u} = \mathbf{A}\mathbf{x} \ \leftrightarrow\ $ coset $\mathcal{L}^{\perp} + \mathbf{x}$



Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

[Leftover hash lemma: $(\mathbf{A}, \mathbf{u} = f_{\mathbf{A}}(U_m))$ is uniform*.]

Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

[Leftover hash lemma: $(\mathbf{A}, \mathbf{u} = f_{\mathbf{A}}(U_m))$ is uniform*.]

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

[Leftover hash lemma: $(\mathbf{A}, \mathbf{u} = f_{\mathbf{A}}(U_m))$ is uniform*.]

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

  ...yields SIS solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

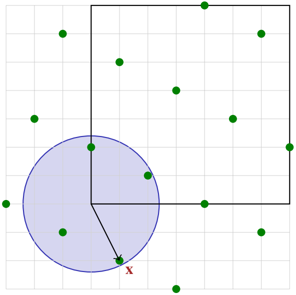
[Leftover hash lemma: $(\mathbf{A}, \mathbf{u} = f_{\mathbf{A}}(U_m))$ is uniform*.]

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

... yields SIS solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

Lattice-Centric Variant

- Domain $\mathbb{Z}^m \cap \text{Ball}(s\sqrt{m})$, input $\mathbf{x} \sim D_{\mathbb{Z}^m,s}$



Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

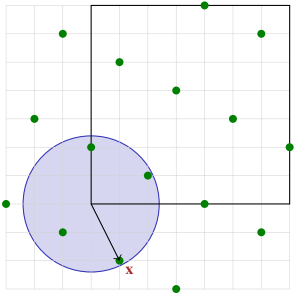
[Leftover hash lemma: $(\mathbf{A}, \mathbf{u} = f_{\mathbf{A}}(U_m))$ is uniform*.]

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

...yields SIS solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

Lattice-Centric Variant

- Domain $\mathbb{Z}^m \cap \text{Ball}(s\sqrt{m})$, input $\mathbf{x} \sim D_{\mathbb{Z}^m,s}$
- Syndrome $\mathbf{u} = f_{\mathbf{A}}(\mathbf{x})$ specifies uniform* coset of $\mathcal{L}^{\perp}(\mathbf{A})$



Application: One-Way / Collision-Resistant Hash

- Let $m > n \lg q$. Define $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

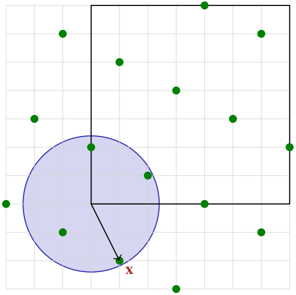
[Leftover hash lemma: $(\mathbf{A}, \mathbf{u} = f_{\mathbf{A}}(U_m))$ is uniform*.]

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

...yields SIS solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

Lattice-Centric Variant

- Domain $\mathbb{Z}^m \cap \text{Ball}(s\sqrt{m})$, input $\mathbf{x} \sim D_{\mathbb{Z}^m, s}$
- Syndrome $\mathbf{u} = f_{\mathbf{A}}(\mathbf{x})$ specifies uniform* coset of $\mathcal{L}^{\perp}(\mathbf{A})$
- Tomorrow: $f_{\mathbf{A}}$ admits natural trapdoor inversion algorithm...



Worst-Case Hardness of SIS

Theorem [Ajtai'96,...,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$$\Downarrow$$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, ... on any n-dim lattice (w/ high prob)

Worst-Case Hardness of SIS

Theorem [Ajtai'96,...,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$\Downarrow$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, ... on any n-dim lattice (w/ high prob)

Proof (simplified for $q = 2\beta\sqrt{n}$)

Given basis $\mathbf{B}$ of any $\mathcal{L}$, where $s = \|\mathbf{B}\| \geq q \cdot \text{smooth}(\mathcal{L})$:

Worst-Case Hardness of SIS

Theorem [Ajtai'96,...,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$\Downarrow$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, ... on any n-dim lattice (w/ high prob)

Proof (simplified for $q = 2\beta\sqrt{n}$)

Given basis $\mathbf{B}$ of any $\mathcal{L}$, where $s = \|\mathbf{B}\| \geq q \cdot \text{smooth}(\mathcal{L})$:

1. Sample $\mathbf{A}$: for $i = 1$ to m:
   - ⋆ Draw $\mathbf{y}_i \sim D_{\mathcal{L},s}$ using sampling algorithm [$s = \|\mathbf{B}\|$]
   - ⋆ Map $\mathbf{y}_i \in \mathcal{L}/q\mathcal{L}$ to $\mathbf{a}_i = \mathbf{B}^{-1}\mathbf{y}_i \in \mathbb{Z}_q^n$ [uniform: $s \geq \text{smooth}(q\mathcal{L})$]

Worst-Case Hardness of SIS

Theorem [Ajtai'96,...,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$$\Downarrow$$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, ... on any n-dim lattice (w/ high prob)

Proof (simplified for $q = 2\beta\sqrt{n}$)

Given basis $\mathbf{B}$ of any $\mathcal{L}$, where $s = \|\mathbf{B}\| \geq q \cdot \text{smooth}(\mathcal{L})$:

1. Sample $\mathbf{A}$: for $i = 1$ to m:
   - ★ Draw $\mathbf{y}_i \sim D_{\mathcal{L},s}$ using sampling algorithm
   - ★ Map $\mathbf{y}_i \in \mathcal{L}/q\mathcal{L}$ to $\mathbf{a}_i = \mathbf{B}^{-1}\mathbf{y}_i \in \mathbb{Z}_q^n$
2. Solve SIS on $\mathbf{A}$: get nonzero $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0} \in \mathbb{Z}_q^n$ and $\|\mathbf{z}\| \leq \beta$.

Worst-Case Hardness of SIS

Theorem [Ajtai'96,...,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$$\Downarrow$$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, ... on any n-dim lattice (w/ high prob)

Proof (simplified for $q = 2\beta\sqrt{n}$)

Given basis $\mathbf{B}$ of any $\mathcal{L}$, where $s = \|\mathbf{B}\| \geq q \cdot \text{smooth}(\mathcal{L})$:

1. Sample $\mathbf{A}$: for $i = 1$ to m:
   - Draw $\mathbf{y}_i \sim D_{\mathcal{L},s}$ using sampling algorithm
   - Map $\mathbf{y}_i \in \mathcal{L}/q\mathcal{L}$ to $\mathbf{a}_i = \mathbf{B}^{-1}\mathbf{y}_i \in \mathbb{Z}_q^n$
2. Solve SIS on $\mathbf{A}$: get nonzero $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0} \in \mathbb{Z}_q^n$ and $\|\mathbf{z}\| \leq \beta$.
3. Combine $\mathbf{y}_i$'s: let $\mathbf{x} = \mathbf{Y}\mathbf{z} \in q\mathcal{L}$. Also, $\mathbf{x} \neq \mathbf{0}$ and $\|\mathbf{x}\| \leq s\beta\sqrt{n}$ (w/hp).

Worst-Case Hardness of SIS

Theorem [Ajtai'96,…,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$\Downarrow$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, …on any n-dim lattice (w/ high prob)

Proof (simplified for $q = 2\beta\sqrt{n}$)

Given basis $\mathbf{B}$ of any $\mathcal{L}$, where $s = \|\mathbf{B}\| \geq q \cdot \text{smooth}(\mathcal{L})$:

1. Sample $\mathbf{A}$: for $i = 1$ to m:
   - ⋆ Draw $\mathbf{y}_i \sim D_{\mathcal{L},s}$ using sampling algorithm
   - ⋆ Map $\mathbf{y}_i \in \mathcal{L}/q\mathcal{L}$ to $\mathbf{a}_i = \mathbf{B}^{-1}\mathbf{y}_i \in \mathbb{Z}_q^n$
2. Solve SIS on $\mathbf{A}$: get nonzero $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{Az} = \mathbf{0} \in \mathbb{Z}_q^n$ and $\|\mathbf{z}\| \leq \beta$.
3. Combine $\mathbf{y}_i$'s: let $\mathbf{x} = \mathbf{Yz} \in q\mathcal{L}$. Also, $\mathbf{x} \neq \mathbf{0}$ and $\|\mathbf{x}\| \leq s\beta\sqrt{n}$ (w/hp).

   $\Rightarrow$ So $\mathbf{x}/q \in \mathcal{L}$ and $\|\mathbf{x}/q\| \leq s/2$. Shorter!

Worst-Case Hardness of SIS

Theorem [Ajtai'96,…,MR'04,GPV'08]

For $q \geq 2\beta\sqrt{n}$, solving SIS w/ length bound β (w/ non-negl prob)

$$\Downarrow$$

Solving $2\beta\sqrt{n}$-GapSVP, -SIVP, …on any n-dim lattice (w/ high prob)

Proof (simplified for $q = 2\beta\sqrt{n}$)

Given basis $\mathbf{B}$ of any $\mathcal{L}$, where $s = \|\mathbf{B}\| \geq q \cdot \text{smooth}(\mathcal{L})$:

1. Sample $\mathbf{A}$: for $i = 1$ to m:
   - ⋆ Draw $\mathbf{y}_i \sim D_{\mathcal{L},s}$ using sampling algorithm
   - ⋆ Map $\mathbf{y}_i \in \mathcal{L}/q\mathcal{L}$ to $\mathbf{a}_i = \mathbf{B}^{-1}\mathbf{y}_i \in \mathbb{Z}_q^n$
2. Solve SIS on $\mathbf{A}$: get nonzero $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{Az} = \mathbf{0} \in \mathbb{Z}_q^n$ and $\|\mathbf{z}\| \leq \beta$.
3. Combine $\mathbf{y}_i$'s: let $\mathbf{x} = \mathbf{Yz} \in q\mathcal{L}$. Also, $\mathbf{x} \neq \mathbf{0}$ and $\|\mathbf{x}\| \leq s\beta\sqrt{n}$ (w/hp).

   $\Rightarrow$ So $\mathbf{x}/q \in \mathcal{L}$ and $\|\mathbf{x}/q\| \leq s/2$. Shorter!

Get a shorter basis $\|\mathbf{B}'\| \leq s/2$. Wash, rinse, repeat…

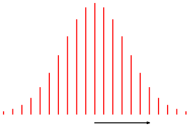
‘Learning With Errors’ (LWE) Problem [Regev’05]

- Generalizes ‘learning parity with noise’ to larger moduli q

‘Learning With Errors’ (LWE) Problem [Regev’05]

- Generalizes ‘learning parity with noise’ to larger moduli q
- <u>**Search**</u>: *find* $\mathbf{s} \in \mathbb{Z}_q^n$, given ‘noisy random inner products’

$$\mathbf{a}_1 \quad , \quad b_1 = \langle \mathbf{a}_1 \ , \ \mathbf{s} \rangle + e_1$$
$$\mathbf{a}_2 \quad , \quad b_2 = \langle \mathbf{a}_2 \ , \ \mathbf{s} \rangle + e_2$$
$$\vdots$$

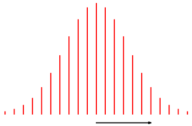


error $\alpha \cdot q \geq 2\sqrt{n}$

‘Learning With Errors’ (LWE) Problem [Regev’05]

- Generalizes ‘learning parity with noise’ to larger moduli q
- **Search:** *find* $\mathbf{s} \in \mathbb{Z}_q^n$, given ‘noisy random inner products’

$$m \left\{ \begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix} \right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

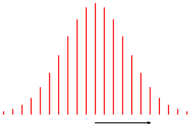


error $\alpha \cdot q \geq 2\sqrt{n}$

‘Learning With Errors’ (LWE) Problem [Regev’05]

- Generalizes ‘learning parity with noise’ to larger moduli q
- **Search:** *find* $\mathbf{s} \in \mathbb{Z}_q^n$, given ‘noisy random inner products’

$$m \left\{ \begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix} \right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t \mathbf{s} + \mathbf{e}$$



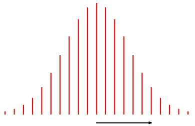
error $\alpha \cdot q \geq 2\sqrt{n}$

- **Decision:** *distinguish* $(\mathbf{A}\ ,\ \mathbf{b})$ from uniform $(\mathbf{A}\ ,\ \mathbf{b})$

‘Learning With Errors’ (LWE) Problem [Regev’05]

- Generalizes ‘learning parity with noise’ to larger moduli q
- **Search:** *find* $\mathbf{s} \in \mathbb{Z}_q^n$, given ‘noisy random inner products’

$$m \left\{ \begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix} \right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$



error $\alpha \cdot q \geq 2\sqrt{n}$

- **Decision:** *distinguish* $(\mathbf{A}\ ,\ \mathbf{b})$ from uniform $(\mathbf{A}\ ,\ \mathbf{b})$

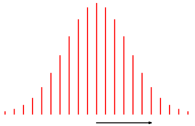
Known Hardness of LWE

- Decision = Search for ‘very smooth’ q [BFKL’93,Regev’05,P’09]

‘Learning With Errors’ (LWE) Problem [Regev’05]

- Generalizes ‘learning parity with noise’ to larger moduli q
- **Search:** *find* $\mathbf{s} \in \mathbb{Z}_q^n$, given ‘noisy random inner products’

$$m \left\{ \begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix} \right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t \mathbf{s} + \mathbf{e}$$



error $\alpha \cdot q \geq 2\sqrt{n}$

- **Decision:** *distinguish* $(\mathbf{A}, \mathbf{b})$ from uniform $(\mathbf{A}, \mathbf{b})$

Known Hardness of LWE

- Decision = Search for ‘very smooth’ q [BFKL’93,Regev’05,P’09]
- Search = (n/α)-approx lattice problems:
  - ⋆ GapSVP & SIVP under *quantum* reduction. [Regev’05]
  - ⋆ GapSVP & variants under *classical* reduction. [P’09] (For large enough q.)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

(Images courtesy xkcd.org)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

$$\xrightarrow[\text{(public key)}]{\mathbf{A},\ \mathbf{u} = \mathbf{A}\mathbf{x}}$$

(Images courtesy xkcd.org)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

$$\xrightarrow{\mathbf{A},\ \mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key)

$$\xleftarrow{\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}}$$

(ciphertext ‘preamble’)

(Images courtesy xkcd.org)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

$\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x}$ →

(public key)

$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$ ←

(ciphertext 'preamble')

$b' + \text{bit} \cdot \lfloor \frac{q}{2} \rfloor$ ←

$b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'$

(key / 'pad')

(Images courtesy xkcd.org)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

$\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x}$ $\longrightarrow$

(public key)

$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$ $\longleftarrow$

(ciphertext ‘preamble’)

$b' + \text{bit} \cdot \lfloor \frac{q}{2} \rfloor$ $\longleftarrow$

$$\langle \mathbf{x}, \mathbf{b} \rangle \approx \mathbf{x}^t\mathbf{A}^t\mathbf{s} = \langle \mathbf{u}, \mathbf{s} \rangle \approx b'$$

$$\boxed{b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'}$$

(key / ‘pad’)

(Images courtesy xkcd.org)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

$\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x}$ →

(public key)

$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$ ←

(ciphertext 'preamble')

$b' + \text{bit} \cdot \lfloor \frac{q}{2} \rceil$ ←

$$\langle \mathbf{x}, \mathbf{b} \rangle \approx \mathbf{x}^t \mathbf{A}^t \mathbf{s} = \langle \mathbf{u}, \mathbf{s} \rangle \approx b'$$

$$\boxed{b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'}$$

(key / 'pad')

? $(\mathbf{A}, \mathbf{u}, \mathbf{b}, b')$

(Images courtesy xkcd.org)

Application: Public-Key Encryption

$\mathbf{x} \in \{0,1\}^m$

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

$\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x}$ $\longrightarrow$

(public key)

$\mathbf{b} = \mathbf{A}^t \mathbf{s} + \mathbf{e}$ $\longleftarrow$

(ciphertext 'preamble')

$b' + \text{bit} \cdot \lfloor \frac{q}{2} \rfloor$ $\longleftarrow$

$$\langle \mathbf{x}, \mathbf{b} \rangle \approx \mathbf{x}^t \mathbf{A}^t \mathbf{s} = \langle \mathbf{u}, \mathbf{s} \rangle \approx b'$$

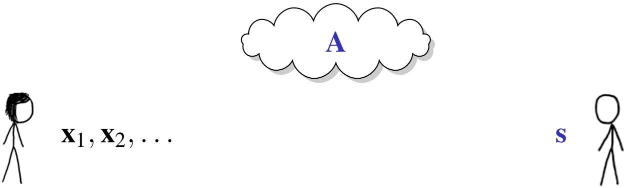
$$\boxed{b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'}$$

(key / 'pad')

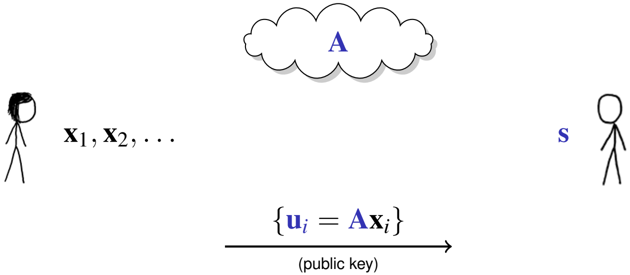
? $(\mathbf{A}, \mathbf{u}, \mathbf{b}, b')$

(Images courtesy xkcd.org)

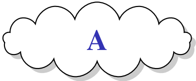
Improved Efficiency



Improved Efficiency



Improved Efficiency



$\mathbf{x}_1, \mathbf{x}_2, \ldots$

$\mathbf{s}$

$\{\mathbf{u}_i = \mathbf{A}\mathbf{x}_i\}$ →

(public key)

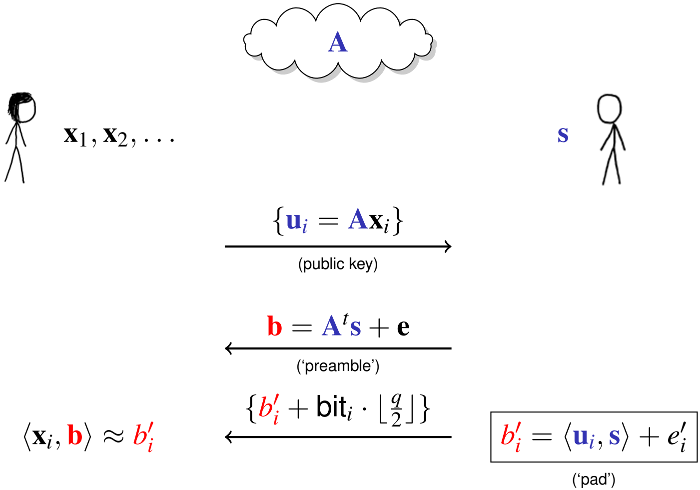
$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$ ←

('preamble')

$\langle \mathbf{x}_i, \mathbf{b} \rangle \approx b'_i$ ← $\{b'_i + \text{bit}_i \cdot \lfloor \frac{q}{2} \rceil\}$ $b'_i = \langle \mathbf{u}_i, \mathbf{s} \rangle + e'_i$

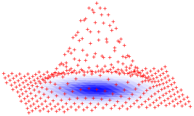
('pad')

Improved Efficiency

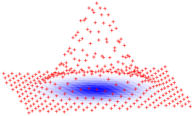


- Tomorrow: some surprising enhancements to this scheme…

Parting Words

1. Discrete Gaussians on lattices are central objects in complexity and cryptography. 

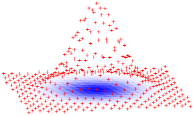
Parting Words

1. Discrete Gaussians on lattices are central objects in complexity and cryptography. 

2. SIS and LWE are the central hard cryptographic problems.

   ⋆ They can be interpreted as both combinatorial and (average-case) lattice problems.

Parting Words

1. Discrete Gaussians on lattices are central objects in complexity and cryptography. 

2. SIS and LWE are the central hard cryptographic problems.
   - ⋆ They can be interpreted as both combinatorial and (average-case) lattice problems.

Thanks!