Worst-Case to Average-Case Reduction for SIS

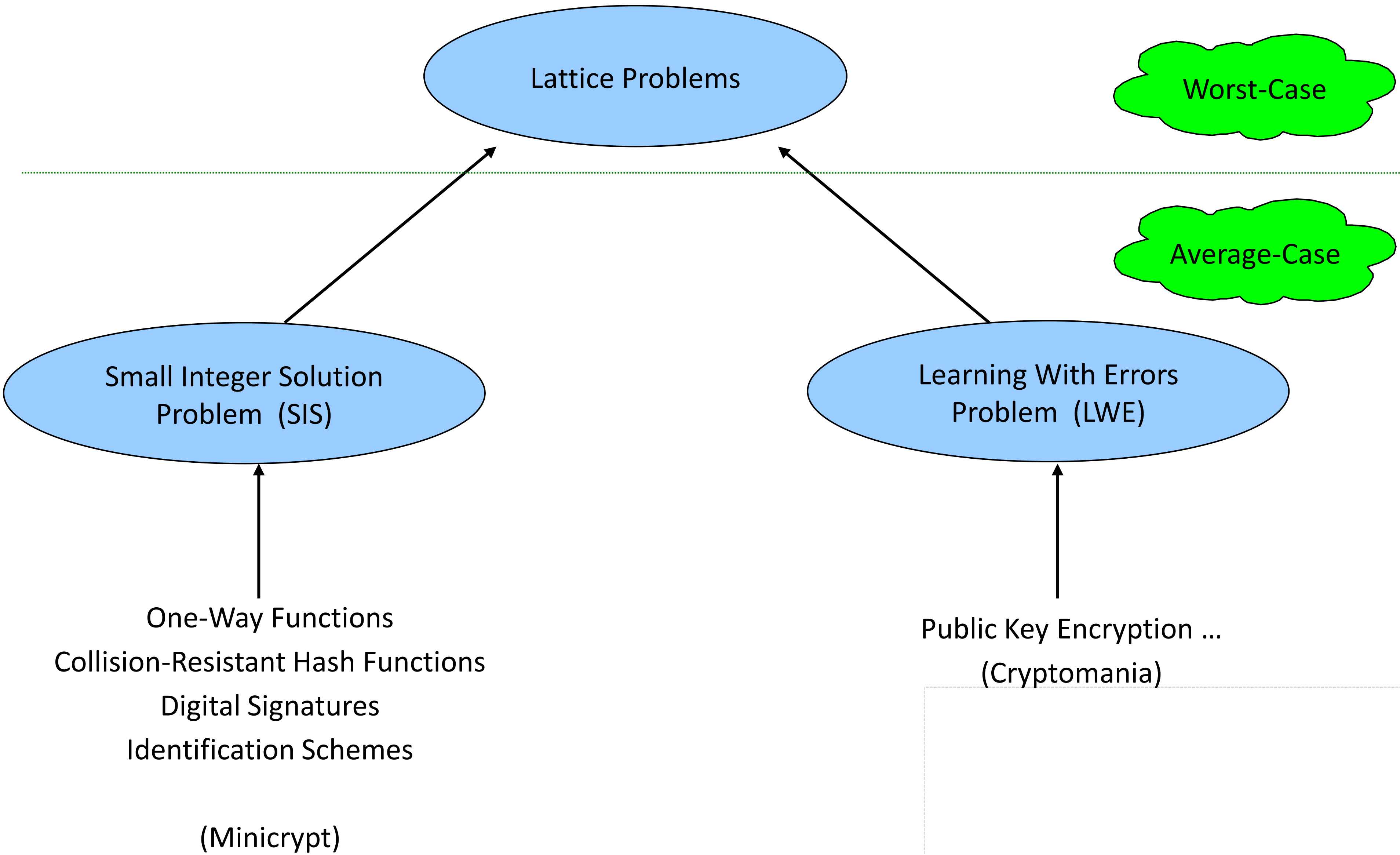
Vadim Lyubashevsky

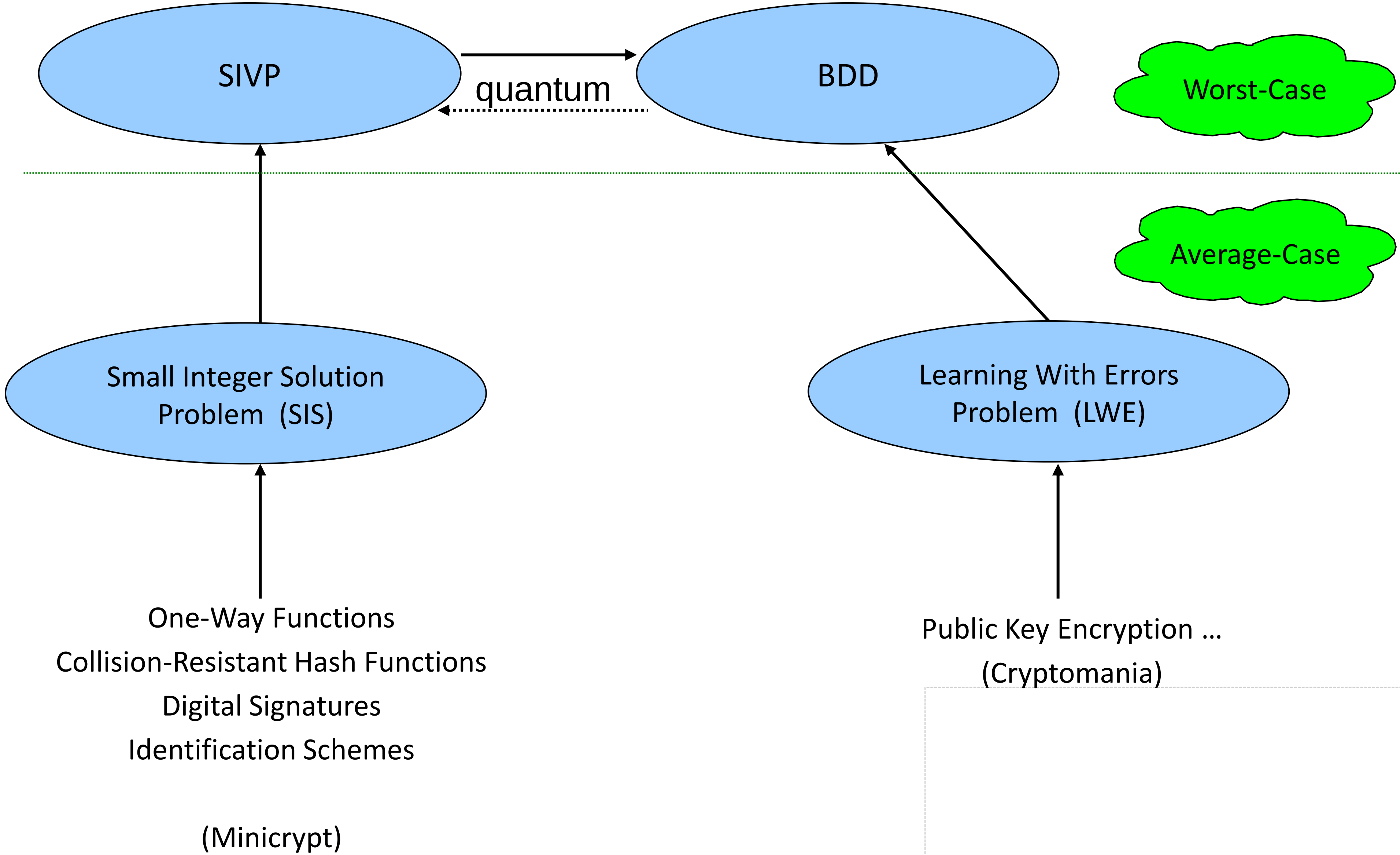
INRIA / ENS, Paris

Session Outline

- Average-Case Problems
  - The Small Integer Solution (SIS) problem
- Gaussian Distributions and Lattices
- Reducing a Worst-Case Lattice Problem to SIS

THE AVERAGE-CASE PROBLEMS


Lattice Problems
Worst-Case
Average-Case
Small Integer Solution Problem (SIS)
Learning With Errors Problem (LWE)
One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes
(Minicrypt)
Public Key Encryption …
(Cryptomania)


SIVP
quantum
BDD
Worst-Case
Average-Case
Small Integer Solution
Problem (SIS)
Learning With Errors
Problem (LWE)
One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes
(Minicrypt)
Public Key Encryption …
(Cryptomania)

Small Integer Solution Problem

Given: Random vectors $a_1,\ldots,a_m$ in $\mathbf{Z}_q^n$

Find: non-trivial solution $z_1,\ldots,z_m$ in $\{-1,0,1\}$ such that

$$z_1 \boxed{a_1} + z_2 \boxed{a_2} + \ldots + z_m \boxed{a_m} = \boxed{0} \quad \text{in } \mathbf{Z}_q^n$$

Observations:

- If size of z_i is not restricted, then the problem is trivial
- Immediately implies a collision-resistant hash function
- A relationship to lattices emerges …

Relationship of SIS to Lattice Problems

Find: non-trivial solution $z_1,\ldots,z_m$ in {-1,0,1} such that

$$z_1 \boxed{a_1} + z_2 \boxed{a_2} + \ldots + z_m \boxed{a_m} = \boxed{0} \quad \text{in } \mathbf{Z}_q^n$$

Let S be the set of all integer $\mathbf{z}=(z_1,\ldots,z_m)$,

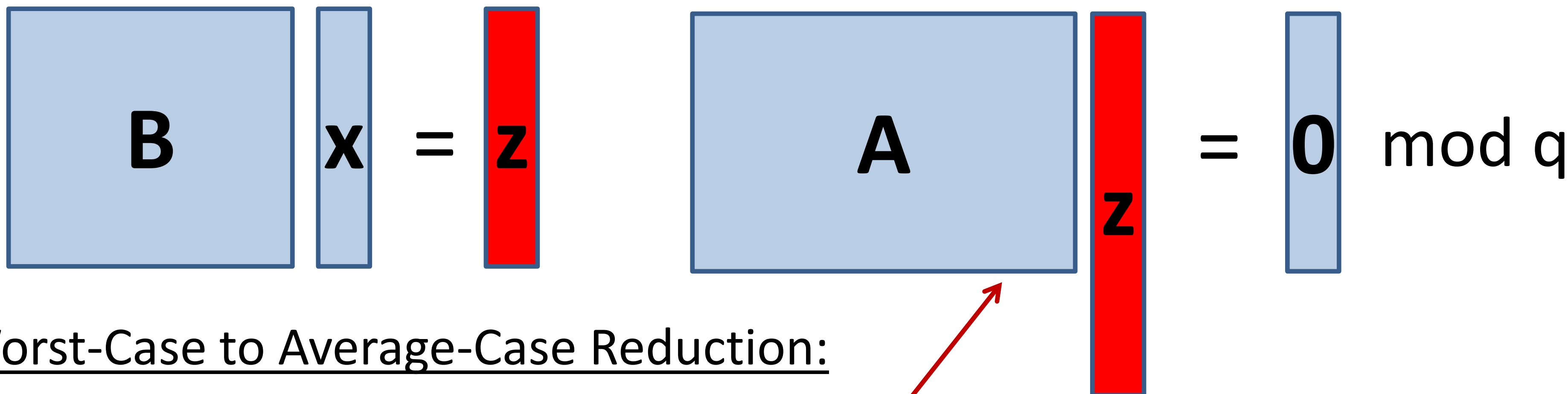
such that $\mathbf{a_1}z_1 + \ldots + \mathbf{a_m}z_m=0 \bmod q$

S is a lattice!

SIS problem asks to find a short vector in S.

Representing Lattices

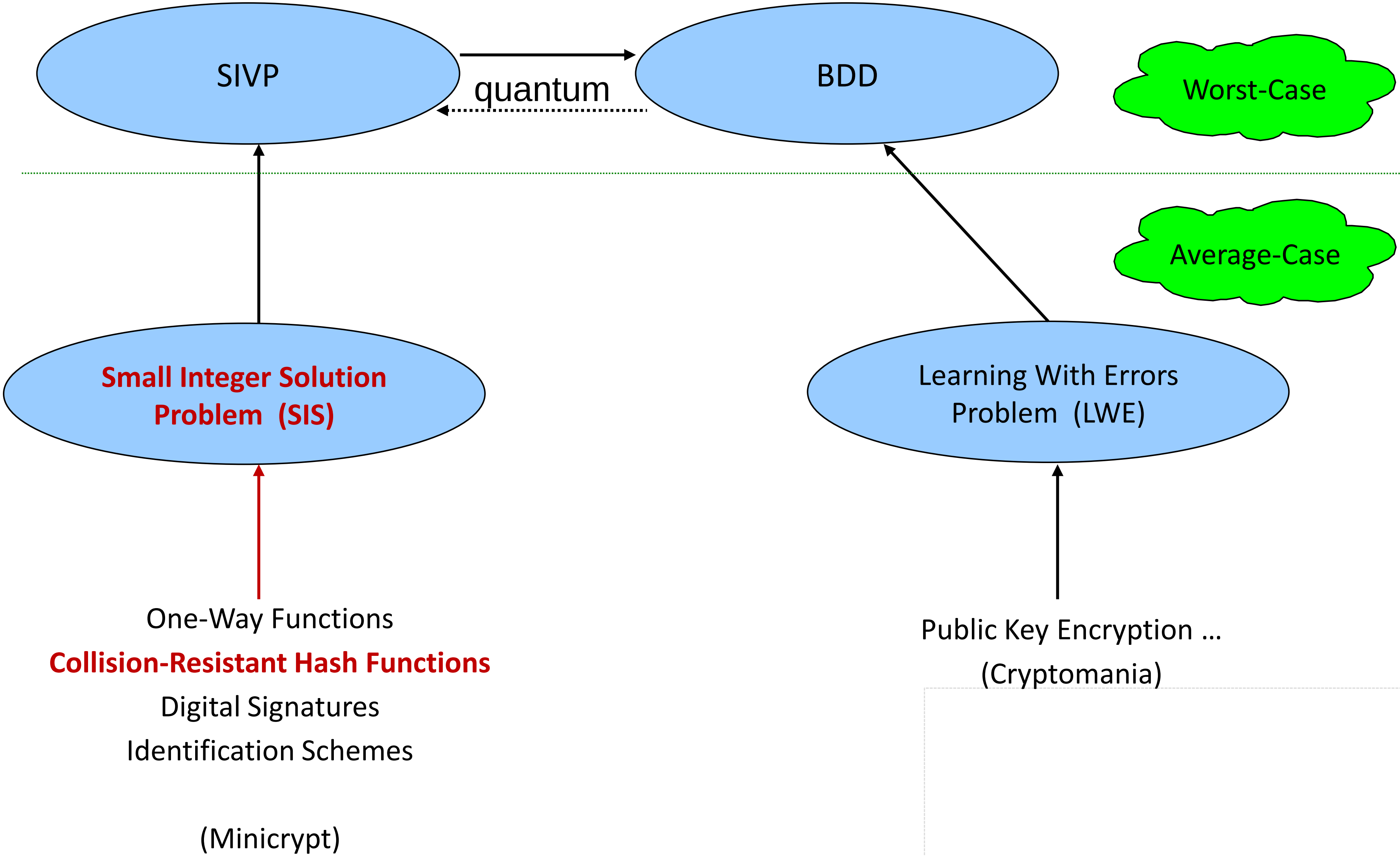
$L(\mathbf{B}) = \{\mathbf{z} : \mathbf{z}=\mathbf{B}\mathbf{x} \text{ for } \mathbf{x} \text{ in } \mathbf{Z}^n\}$ $\quad$ $L^{\perp}(\mathbf{A}) = \{\mathbf{z} \text{ in } \mathbf{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0} \bmod q\}$



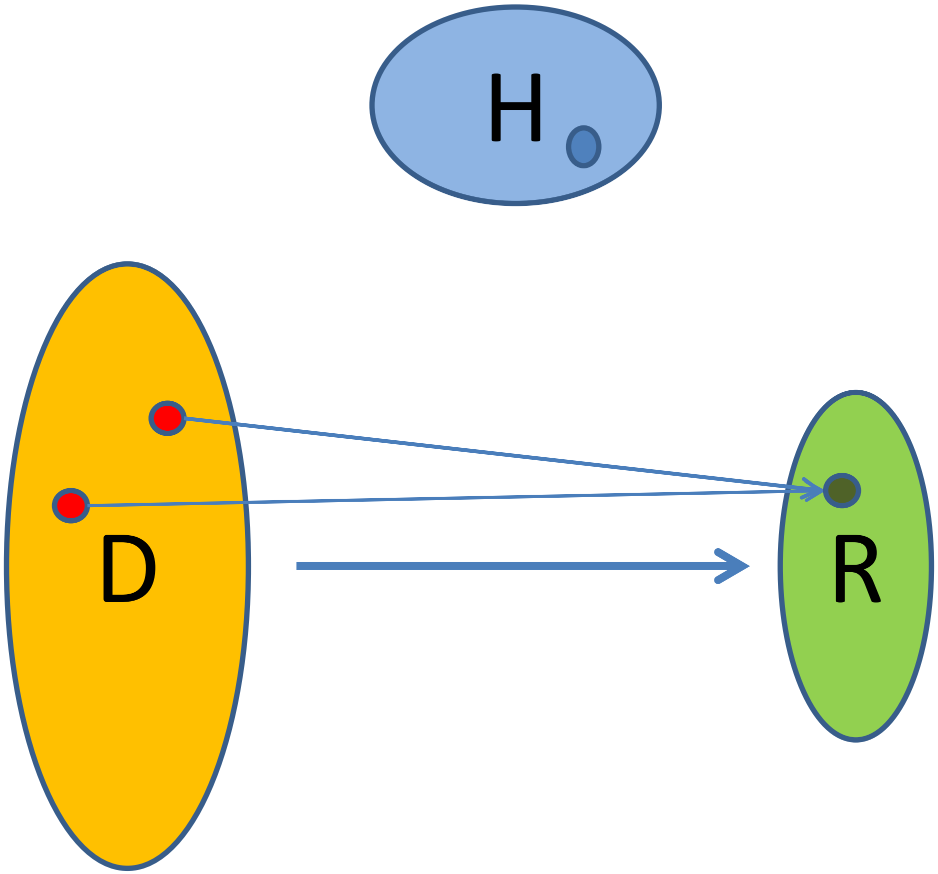
<u>Worst-Case to Average-Case Reduction:</u>

Approximately solving SIVP in all lattices
< Finding short vectors in these lattices

$(m \approx n\log n)$


SIVP
quantum
BDD
Worst-Case
Average-Case
Small Integer Solution Problem (SIS)
Learning With Errors Problem (LWE)
One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes
(Minicrypt)
Public Key Encryption …
(Cryptomania)

Collision-Resistant Hash Functions



For a random h in H,
It is hard to find:

x_1, x_2 in D

such that

$h(x_1) = h(x_2)$

Collision-Resistant Hash Function

Given: Random vectors $a_1,\ldots,a_m$ in $\mathbf{Z}_q^n$

Find: non-trivial solution $z_1,\ldots,z_m$ in {-1,0,1} such that

$$z_1 \boxed{a_1} + z_2 \boxed{a_2} + \ldots + z_m \boxed{a_m} = \boxed{0} \quad \text{in } \mathbf{Z}_q^n$$

$\mathbf{A}=(\mathbf{a_1},\ldots,\mathbf{a_m})$ Define $h_{\mathbf{A}}: \{0,1\}^m \to \mathbf{Z}_q^n$ where

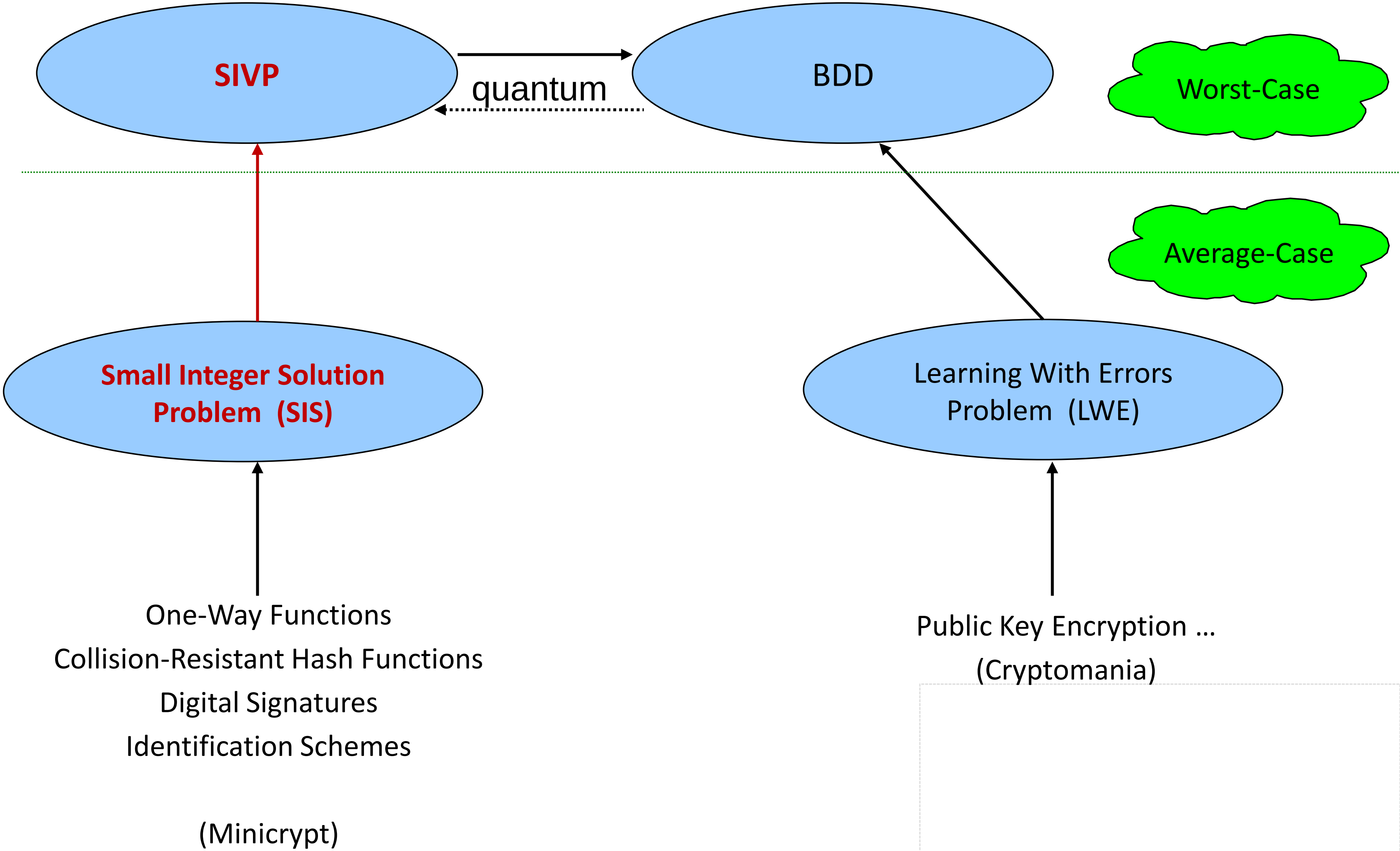
$h_{\mathbf{A}}(\mathbf{z_1},\ldots,\mathbf{z_m})=\mathbf{a_1}z_1 + \ldots + \mathbf{a_m}z_m$

Domain of h = $\{0,1\}^m$ (size = 2^m) Range of h = $\mathbf{Z}_q^n$ (size = q^n)

Set m>nlog q to get compression

Collision: $\mathbf{a_1}z_1 + \ldots + \mathbf{a_m}z_m = \mathbf{a_1}y_1 + \ldots + \mathbf{a_m}y_m$

So, $\mathbf{a_1}(z_1-y_1) + \ldots + \mathbf{a_m}(z_m-y_m) = 0$ and z_i-y_i are in {-1,0,1}


SIVP
quantum
BDD
Worst-Case
Average-Case
Small Integer Solution Problem (SIS)
Learning With Errors Problem (LWE)
One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes
(Minicrypt)
Public Key Encryption …
(Cryptomania)

THE GAUSSIAN (NORMAL) DISTRIBUTION

Definition

1-dimensional Gaussian distribution:

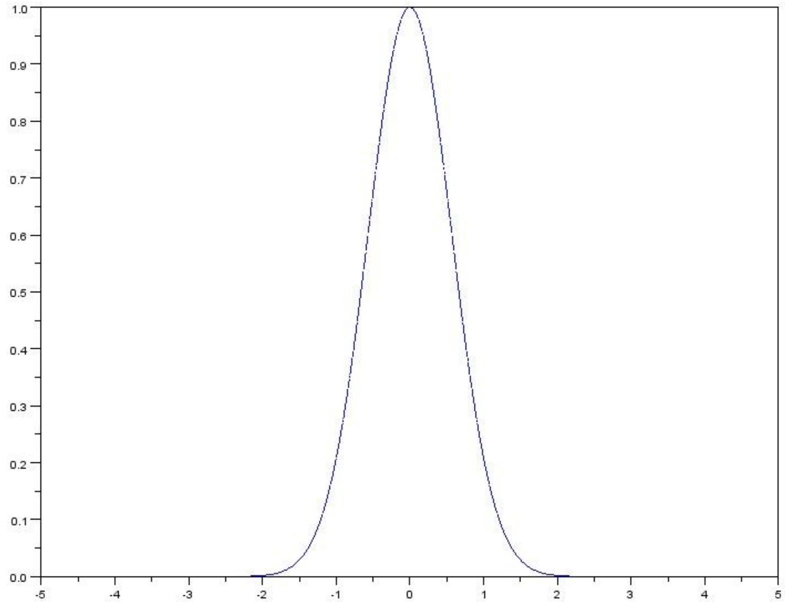
$$\rho_s(x) = (1/s)e^{-\pi x^2/s^2}$$

It's a Normal distribution:

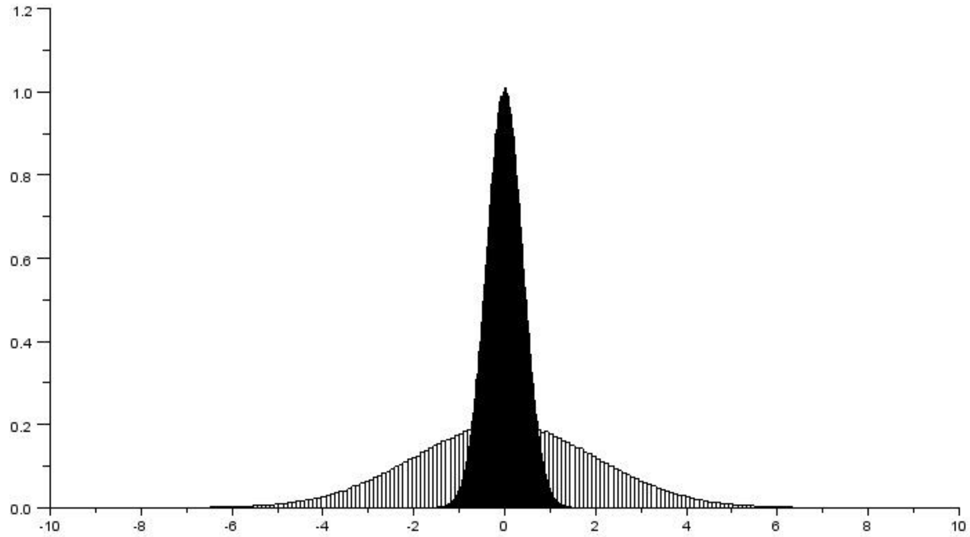
Centered at 0

Standard deviation: $s/\sqrt{2\pi}$

Example (s=1)



Example (s=1 and 5)



2-Dimensional Gaussian

1-dim gaussian on the x_1 axis:

$$\rho_s(x_1) = (1/s)e^{-\pi x_1^2/s^2}$$

1-dim gaussian on the x_2 axis:

$$\rho_s(x_2) = (1/s)e^{-\pi x_2^2/s^2}$$

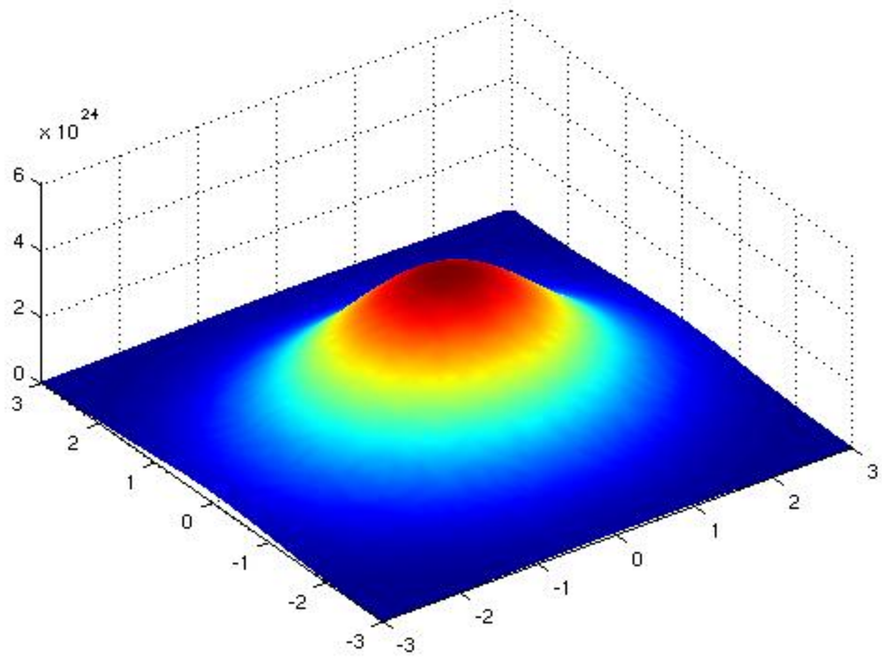
$$\rho_s(x_1,x_2) = \rho_s(x_1) \cdot \rho_s(x_2)$$

$$= (1/s)e^{-\pi x_1^2/s^2} \cdot (1/s)e^{-\pi x_2^2/s^2}$$

$$= (1/s)^2\, e^{-\pi(x_1^2 + x_2^2)/s^2}$$

$$\rho_s(\mathbf{x}) = (1/s)^2\, e^{-\pi\|\mathbf{x}\|^2/s^2}$$

2-Dimensional Example



n-Dimensional Gaussian

n-dimensional Gaussian distribution:

$$\rho_s(\mathbf{x}) = (1/s)^n \, e^{-\pi \|\mathbf{x}\|^2/s^2}$$

It's an n-dimensional Normal distribution:

Centered at **0**

Standard deviation: $s/\sqrt{2\pi}$

Useful Properties of the Gaussian Distribution

1. It is a *Product Distribution*

2. It is *Spherically-Symmetric*

3. It is "uniform" modulo parallelepipeds

Product Distribution

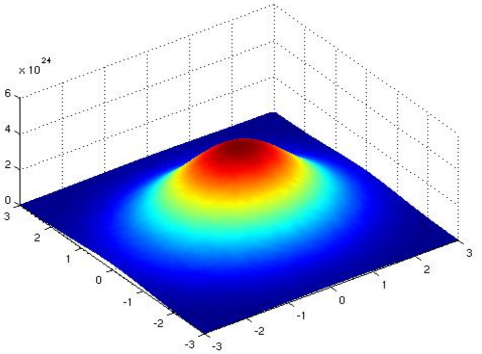
$$\rho_s(\mathbf{x}) = \rho_s(x_1) \cdot \ldots \cdot \rho_s(x_n)$$

Spherically Symmetric

$$\rho_s(\mathbf{x}) = (1/s)^n \, e^{-\pi \|\mathbf{x}\|^2/s^2}$$

The probability of **x** only depends on its length

The distribution is "axis-independent"



Generating Uniform Elements on a Line Segment

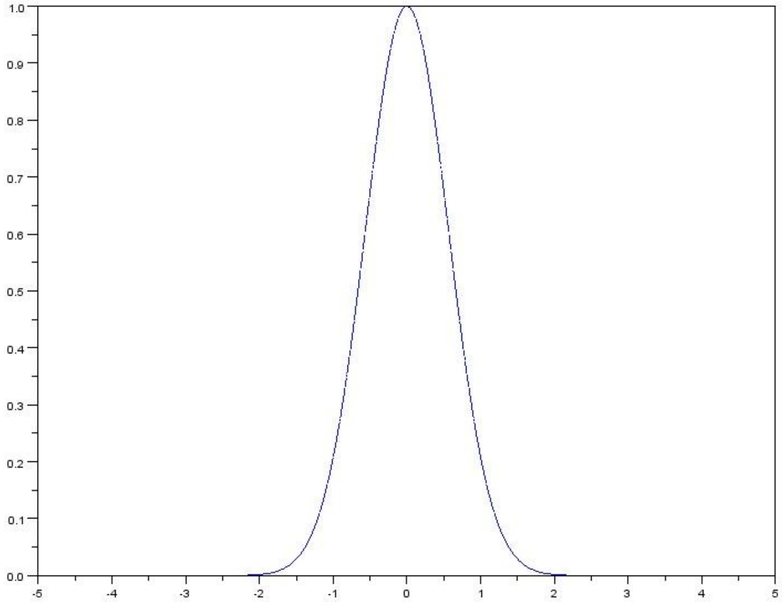
$\rho_s(x) = (1/s)e^{-\pi x^2/s^2}$

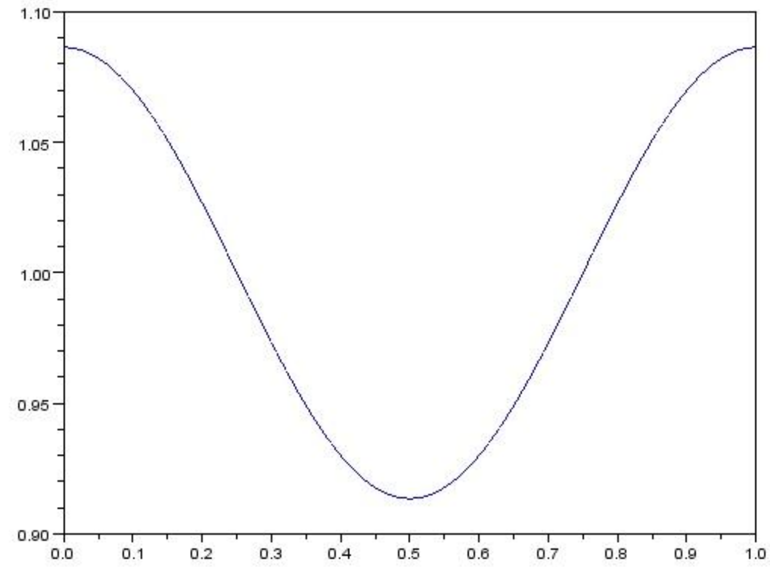
and s=5M, for some positive M

if $X \sim \rho_s$, then for all $m < M$,

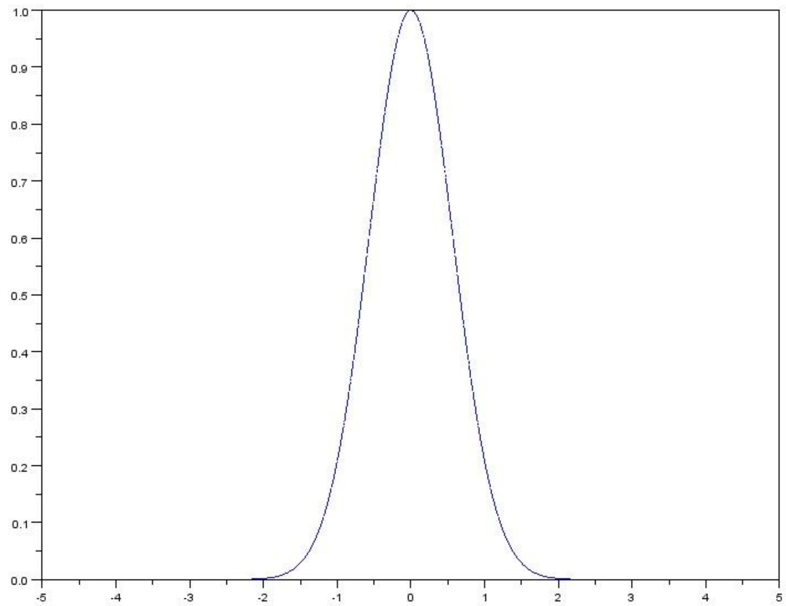
$\Delta\,(X \bmod m\ ,\ \text{Uniform}\ [0, m)\ ) < 2^{-110}$

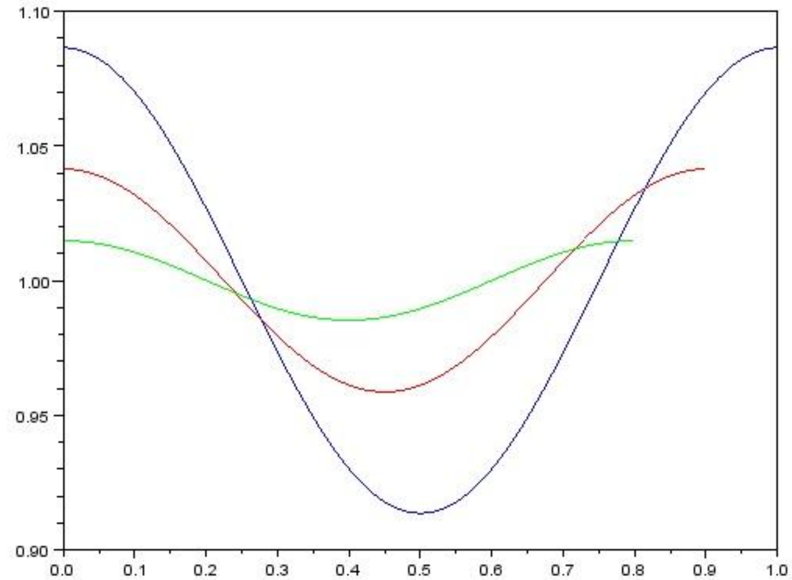
Example (s=1,m=1)



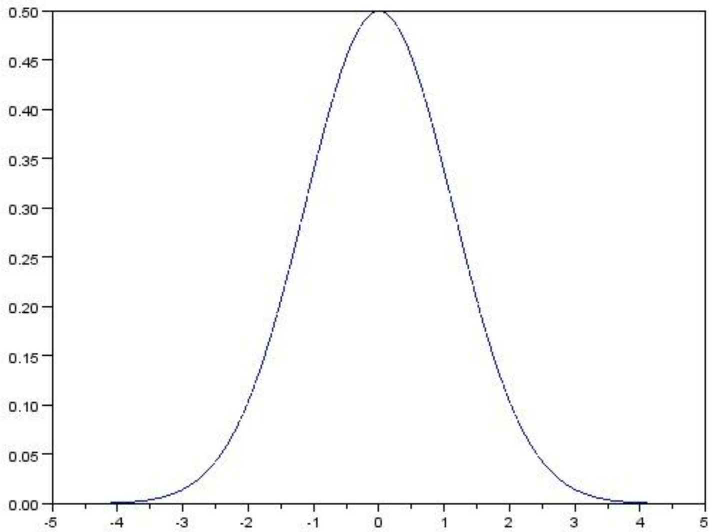


Example (s=1,m=1, .9, .8)

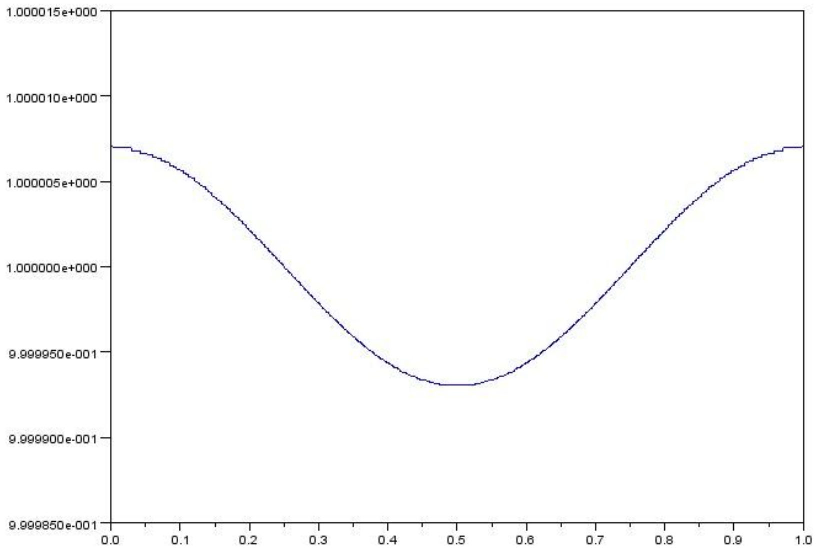




Example (s=2)

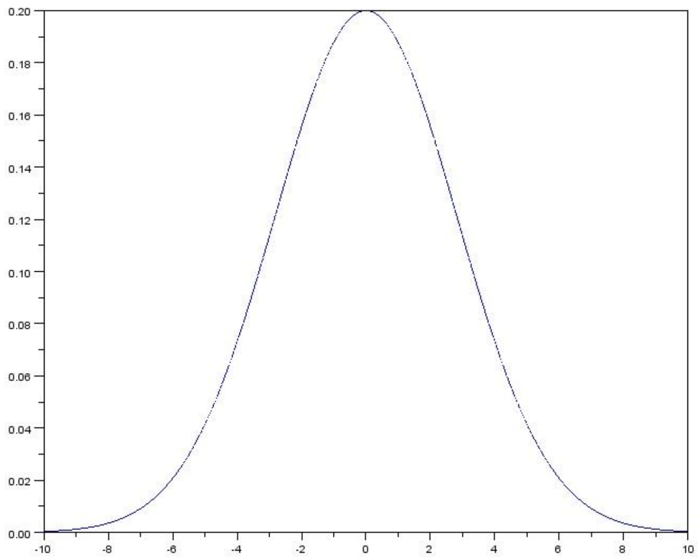


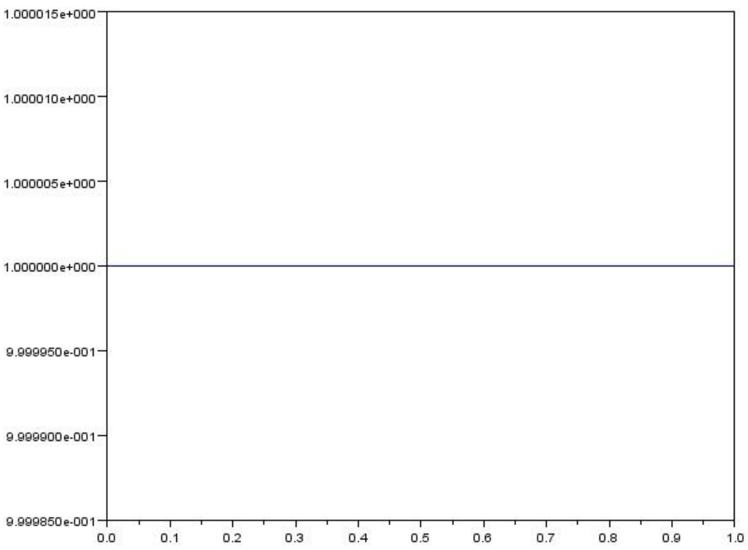
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
-5
-4
-3
-2
-1
0
1
2
3
4
5



1.000015e+000
1.000010e+000
1.000005e+000
1.000000e+000
9.999950e-001
9.999900e-001
9.999850e-001
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0

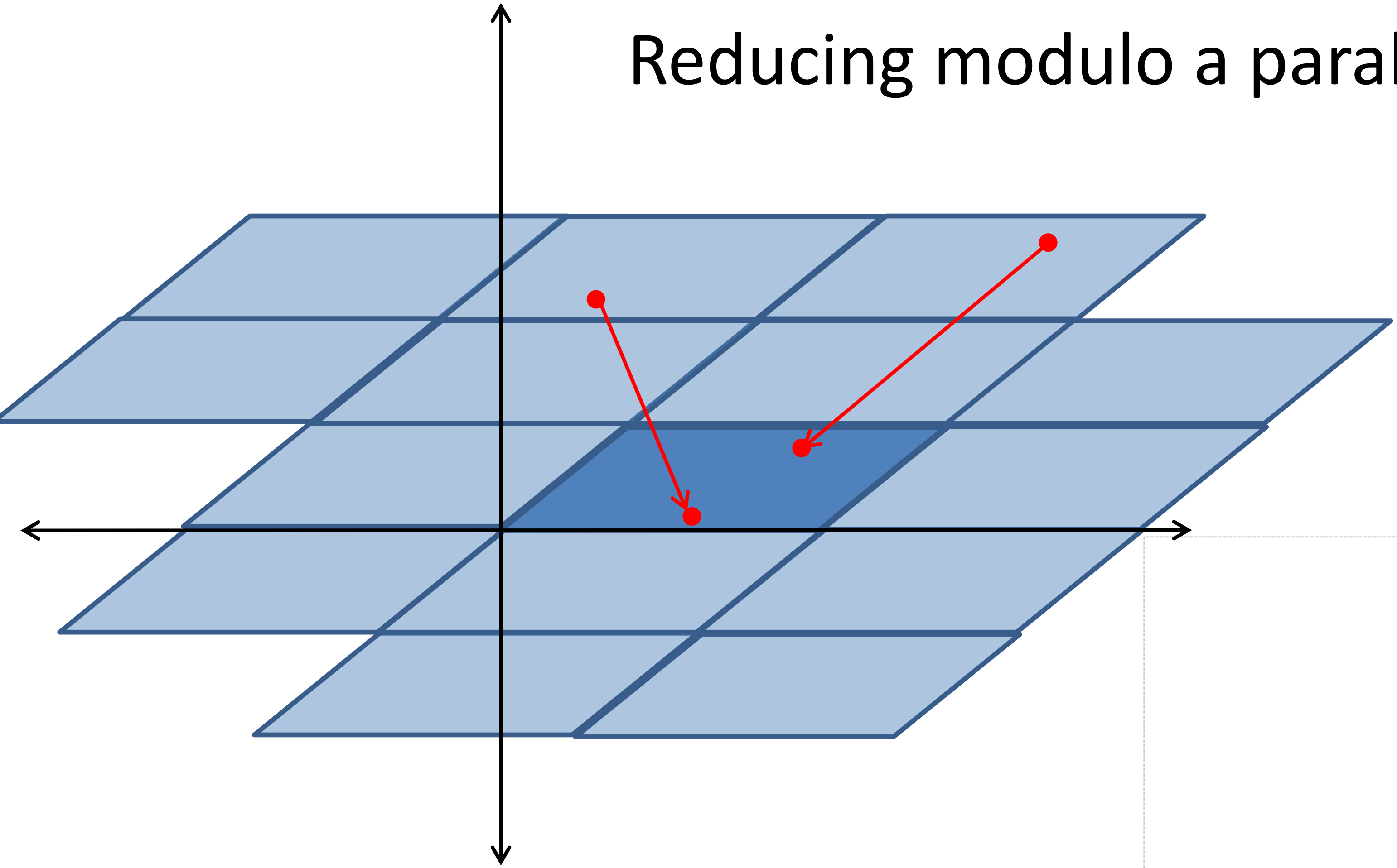
Example (s=5, m=1)





Generating Uniform Elements in an n-dimensional Parallelepiped

Reducing modulo a parallelepiped



Generating Uniform Elements in an n-Dimensional Box

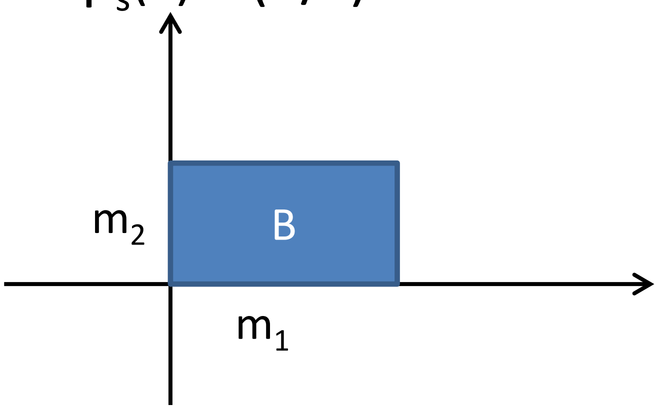
Box **B** with dimensions $(m_1, \ldots, m_n)$, all $m_i < M$.

Generate $X_1, \ldots, X_n \sim \rho_s(x) = (1/s)e^{-\pi x^2/s^2}$, where $s=5M$

For each j, $\Delta(X_j \bmod m,\ \text{Uniform}\ [0, m_j)\ ) < 2^{-110}$

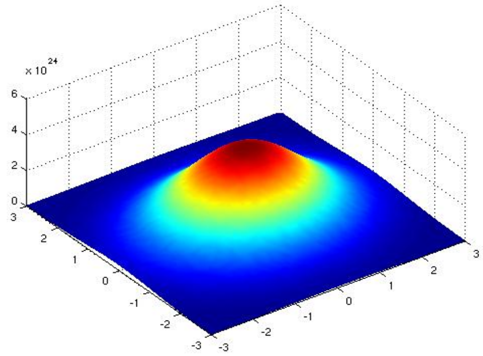
Thus $\Delta((X_1 \bmod m_1, \ldots, X_n \bmod m_n),\ \text{Uniform}(\mathbf{B})) < n2^{-110}$

So, if $\mathbf{X} \sim \rho_s(\mathbf{x}) = (1/s)^n\, e^{-\pi \|\mathbf{x}\|^2/s^2}$ for $s=5M$, $\Delta(\mathbf{X} \bmod \mathbf{B},\ \text{Uniform}(\mathbf{B})) < n2^{-110} \approx 0$

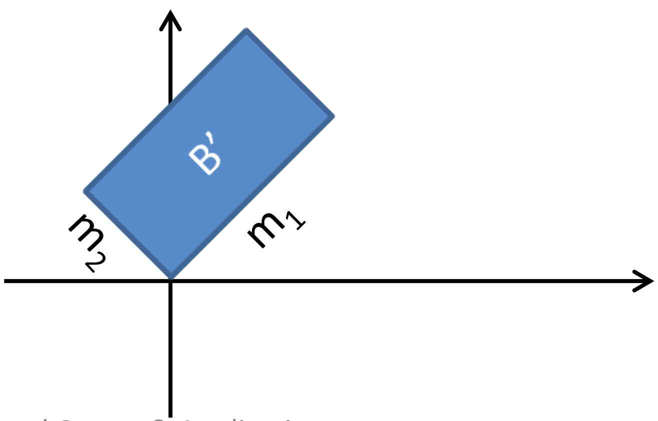


Generating Uniform Elements in a Rotated n-Dimensional Box

$\rho_s(\mathbf{x}) = (1/s)^n\, e^{-\pi\|\mathbf{x}\|^2/s^2}$ is a spherical distribution

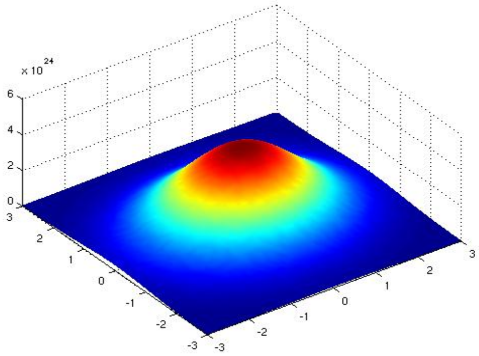


So rotating axes doesn't affect it



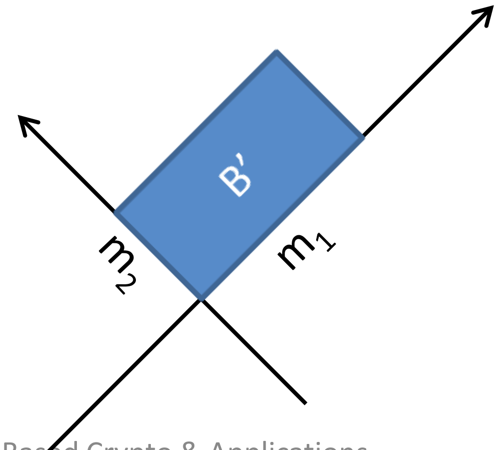
Generating Uniform Elements in a Rotated n-Dimensional Box

$\rho_s(\mathbf{x}) = (1/s)^n e^{-\pi\|\mathbf{x}\|^2/s^2}$ is a spherical distribution



So rotating axes doesn't affect it

Thus, $\Delta(\mathbf{X} \bmod \mathbf{B'}, \text{Uniform}(\mathbf{B'})) \approx 0$



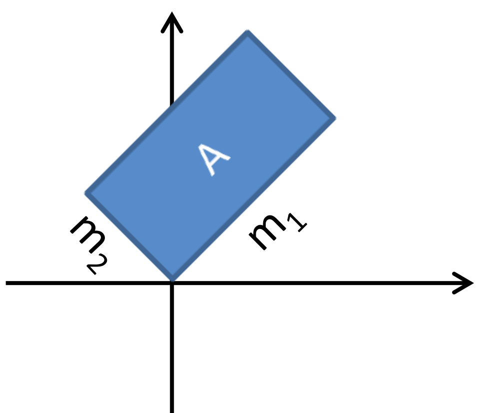
Generating Uniform Elements in Parallelepipeds

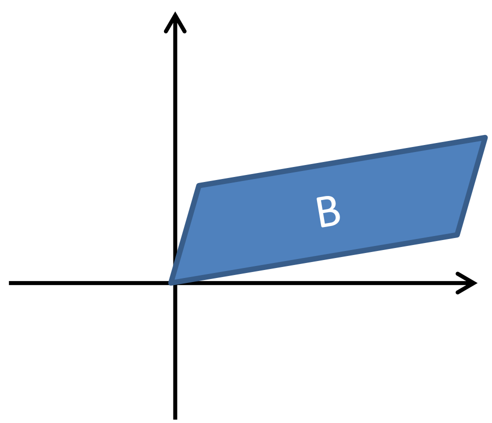
Suppose we have $\mathbf{X} \sim \rho_s(\mathbf{x}) = (1/s)^n\, e^{-\pi\|\mathbf{x}\|^2/s^2}$

and

$\mathbf{X}$ mod $\mathbf{A}$ is uniform

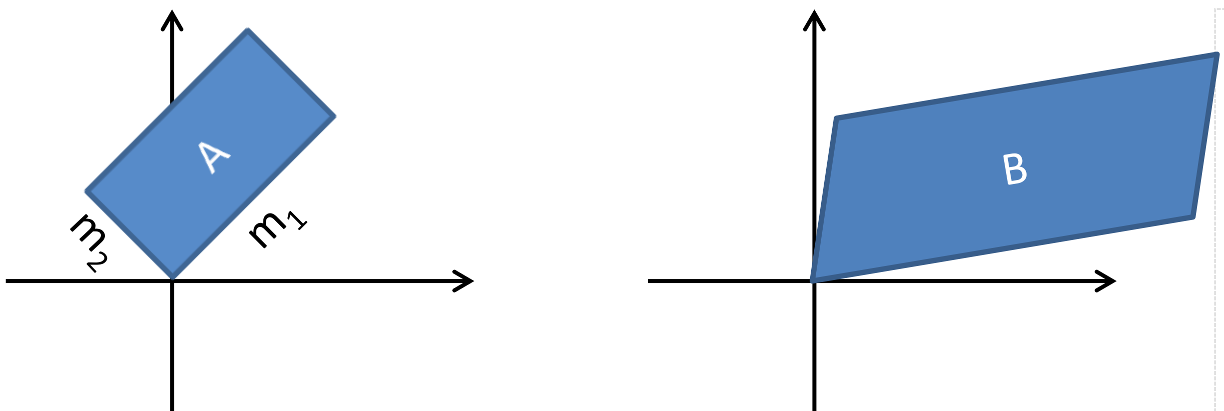
Is $\mathbf{X}$ uniform modulo $\mathbf{B}$?





Generating Uniform Elements in Parallelepipeds

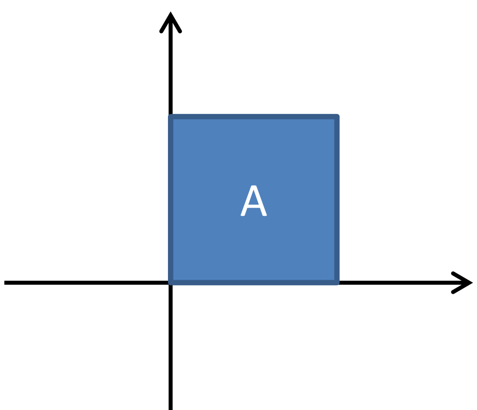
If **B** is much bigger than **A** (i.e. has a bigger determinant), then probably NO.



Generating Uniform Elements in Parallelepipeds

If **B** is much bigger than **A** (i.e. has a bigger determinant), then probably NO.

But what if **B**=**AU** when det(**U**)=1?
Still … not necessarily.



Generating Uniform Elements in Parallelepipeds

If **B**=**AU** and det(**U**)=1, then

X mod **A** is uniform → **X** mod **B** is uniform if:

1.) **U** is an integer matrix or

2.) **U** is an upper-triangular matrix with 1's on the diagonal

Some Simplifying Assumptions

Pretend that the space $\mathbf{R}^n$ is divided into a very very fine grid.

Any two parallelepipeds that have the same determinant have the same number of grid points inside them.

1-to-1 Relationship Between $\mathbf{R}^n$ / $\mathbf{A}$ and $\mathbf{R}^n$ / $\mathbf{B}$

$\mathbf{B} = \mathbf{AU}$

By our assumption $\#(\mathbf{R}^n / \mathbf{A}) = \#(\mathbf{R}^n / \mathbf{B})$

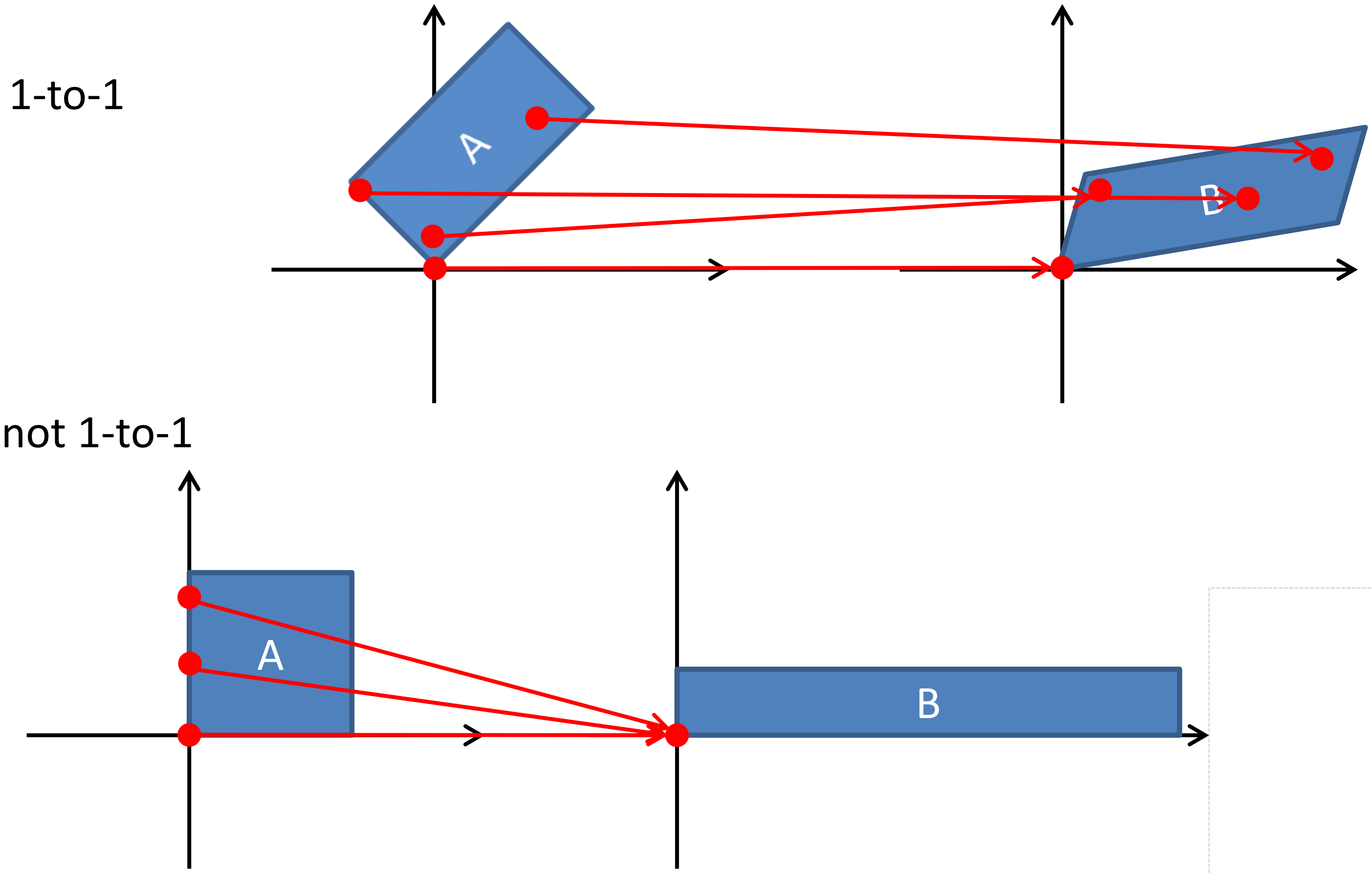
We will now show that:

For every $\mathbf{a}=\mathbf{Az}$, where $\mathbf{z}$ in $[0,1)^n$, $\mathbf{a}$ mod $\mathbf{B}$ is distinct

This implies that if $\mathbf{X}$ mod $\mathbf{A}$ is uniform, then

$\mathbf{X}$ mod $\mathbf{B}$ is uniform too.

1-to-1 Relationship Between $\mathbf{R}^n$ / **A** and $\mathbf{R}^n$ / **B**



1-to-1 Relationship Between $\mathbf{R}^n$ / $\mathbf{A}$ and $\mathbf{R}^n$ / $\mathbf{B}$

If $\mathbf{B}=\mathbf{AU}$ and $\det(\mathbf{U})=1$, then

$\mathbf{X}$ mod $\mathbf{A}$ is uniform $\rightarrow$ $\mathbf{X}$ mod $\mathbf{B}$ is uniform if:

1.) $\mathbf{U}$ is an integer matrix

Then $L(\mathbf{A}) = L(\mathbf{B})$, thus …

If $\mathbf{Az_1}$ mod $\mathbf{B}$ = $\mathbf{Az_2}$ mod $\mathbf{B}$, then

$\mathbf{A}(\mathbf{z_1}-\mathbf{z_2})=0$ mod $\mathbf{B}$

$\mathbf{A}(\mathbf{z_1}-\mathbf{z_2})$ is in $L(\mathbf{B})$

$\mathbf{z_1}-\mathbf{z_2}$ is an integer vector

$\mathbf{z_1}-\mathbf{z_2} = \mathbf{0}$ $\rightarrow\leftarrow$

1-to-1 Relationship Between $\mathbf{R}^n$ / **A** and $\mathbf{R}^n$ / **B**

If **B**=**AU** and det(**U**)=1, then

X mod **A** is uniform → **X** mod **B** is uniform if:

2.) **U** is an upper-triangular matrix with 1's on the diagonal

If $\mathbf{Az}_1$ mod **B** = $\mathbf{Az}_2$ mod **B**, then

$\mathbf{A}(\mathbf{z}_1\text{-}\mathbf{z}_2)=0$ mod **B**

$\mathbf{BU}^{-1}(\mathbf{z}_1\text{-}\mathbf{z}_2)$ is in L(**B**)

$\mathbf{U}^{-1}(\mathbf{z}_1\text{-}\mathbf{z}_2)$ is an integer vector

why? $\mathbf{z}_1\text{-}\mathbf{z}_2 = \mathbf{0}$ →←

1-to-1 Relationship Between $\mathbf{R}^n$ / **A** and $\mathbf{R}^n$ / **B**

U is an upper-triangular matrix with 1's on the diagonal

Thus $\mathbf{U}^{-1}$ is also.

$$\underbrace{\begin{bmatrix} 1 & a & b & \ldots & c \\ 0 & 1 & d & \ldots & e \\ \ldots & 0 & 1 & \ldots & f \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}}_{\mathbf{U}^{-1}} \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \\ \ldots \\ 0 \end{bmatrix}}_{\mathbf{z}_1 - \mathbf{z}_2} = \underbrace{\begin{bmatrix} \\ \\ \\ \\ \end{bmatrix}}_{\text{integer vector}}$$

The Gram-Schmidt Matrix

B is a basis for a lattice

Then $\mathbf{B} = \tilde{\mathbf{B}}\mathbf{U}$ where $\tilde{\mathbf{B}}$ is the Gram-Schmidt basis

$$\underbrace{\begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \tilde{\mathbf{b}}_3 & \cdots & \tilde{\mathbf{b}}_n \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix}}_{\tilde{\mathbf{B}}} \underbrace{\begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & \cdots & \mu_{n,2} \\ \cdots & 0 & 1 & \cdots & \mu_{n,3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}}_{\mathbf{U}} = \mathbf{B}$$

Generating Uniform Elements in Parallelepipeds

Suppose we have **X** $\sim \rho_s(\mathbf{x}) = (1/s)^n e^{-\pi\|\mathbf{x}\|^2/s^2}$

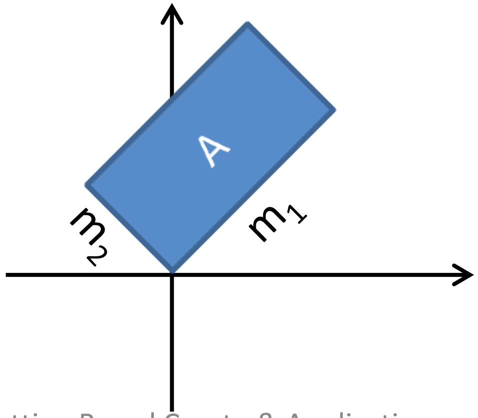
and

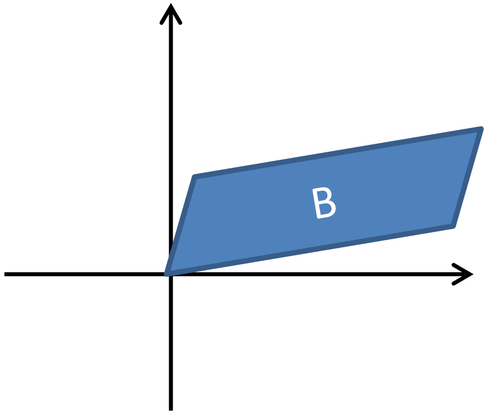
X mod **A** is uniform

Is **X** uniform modulo **B**?

If **A** is the Gram-Schmidt basis of **B**, then YES!

So s needs to be big enough to make **X** uniform mod **A**

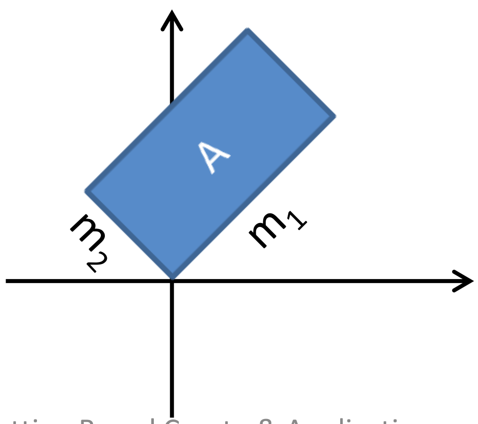


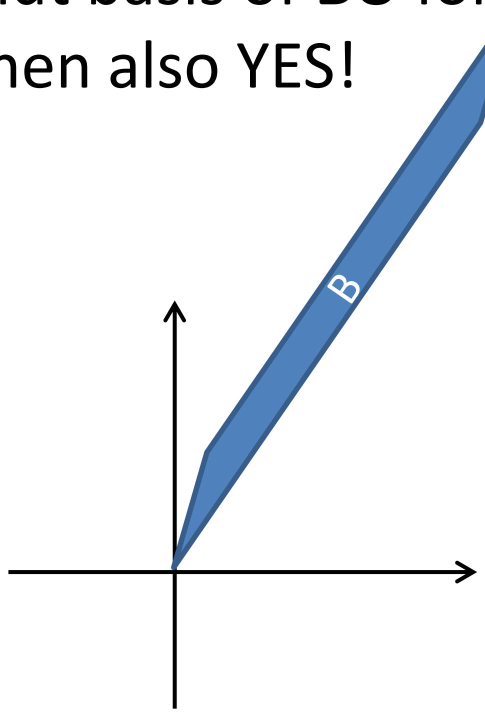


There is more …

X mod **A** is uniform
Is **X** uniform modulo **B**?

If **A** is the Gram-Schmidt basis of **BU** for any integer matrix **U** with determinant 1, then also YES!

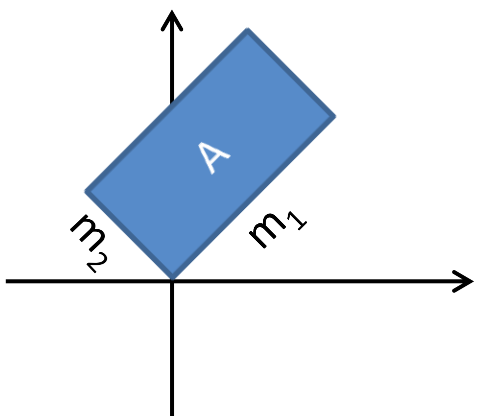


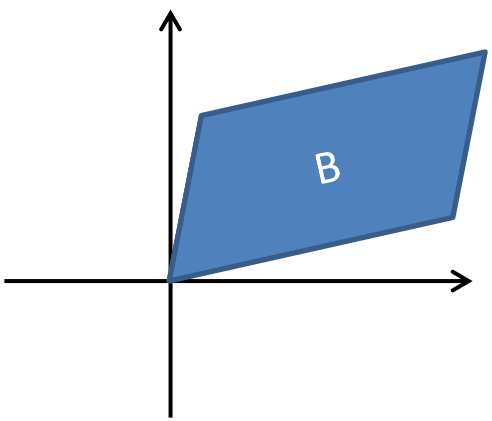


And still more …

X mod **A** is uniform
Is **X** uniform modulo **B**?

If **A** is the Gram-Schmidt basis of **BU** for any integer matrix **U**, then also YES!
(This is because L(**BU**) is a sublattice of L(**B**), and so uniform modulo **BU** implies uniform modulo **B**.)





And in particular …

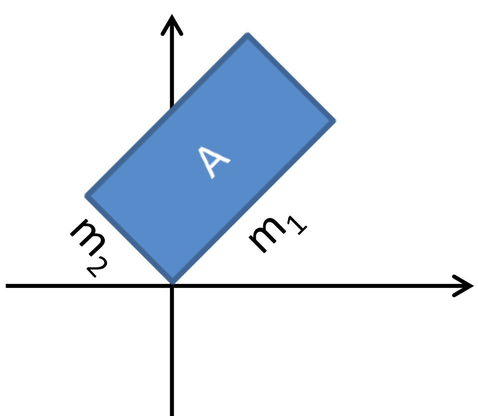
B is a lattice basis

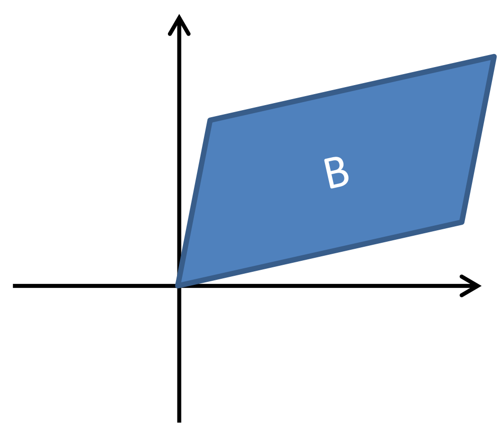
C=**BU** is a (sub)-lattice basis such that all vectors of **C** are at most $\lambda_n(\mathbf{B})$

Then all vectors of $\tilde{\mathbf{C}}$ are of length at most $\lambda_n(\mathbf{B})$

So if $s > 5\lambda_n(\mathbf{B})$, and $\mathbf{X} \sim \rho_s(\mathbf{x}) = (1/s)^n e^{-\pi|\mathbf{x}|^2/s^2}$,then:

$\mathbf{X}$ is uniform mod $\tilde{\mathbf{C}}$ → uniform mod **C** → uniform mod **B**





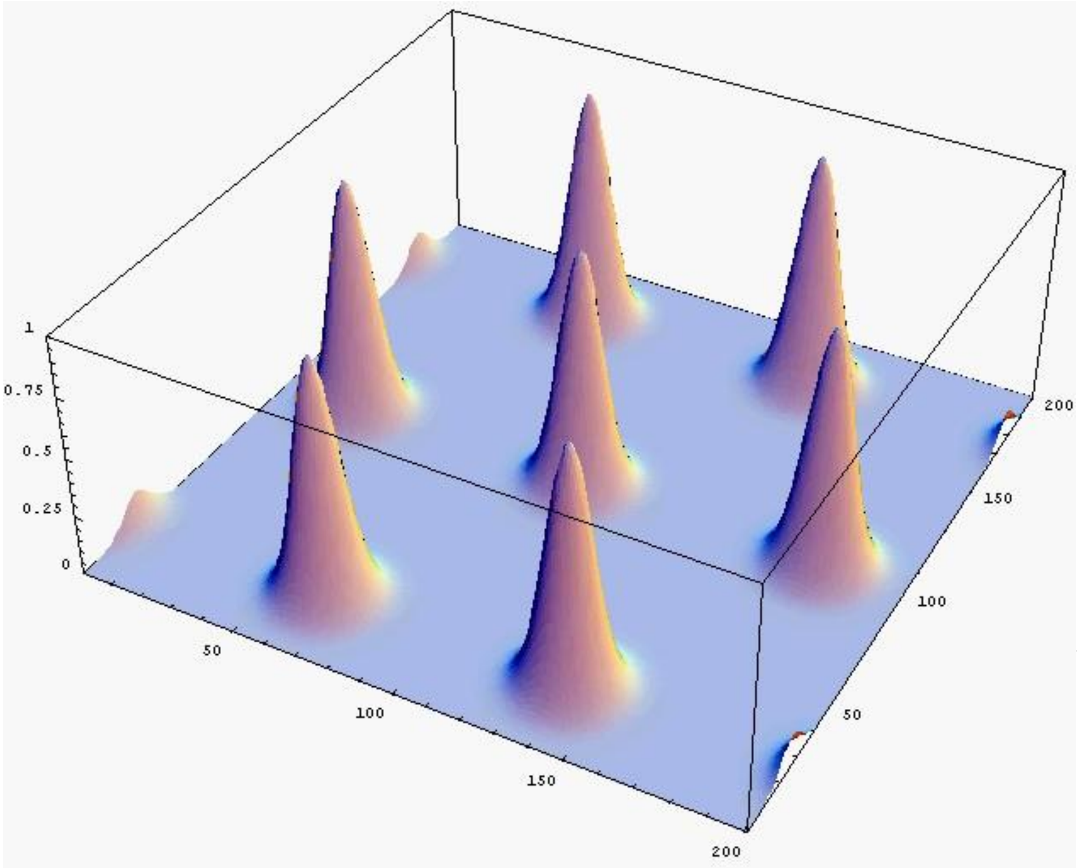
Uniform Distribution Over Lattices

Theorem [Micciancio and Regev 2004]:

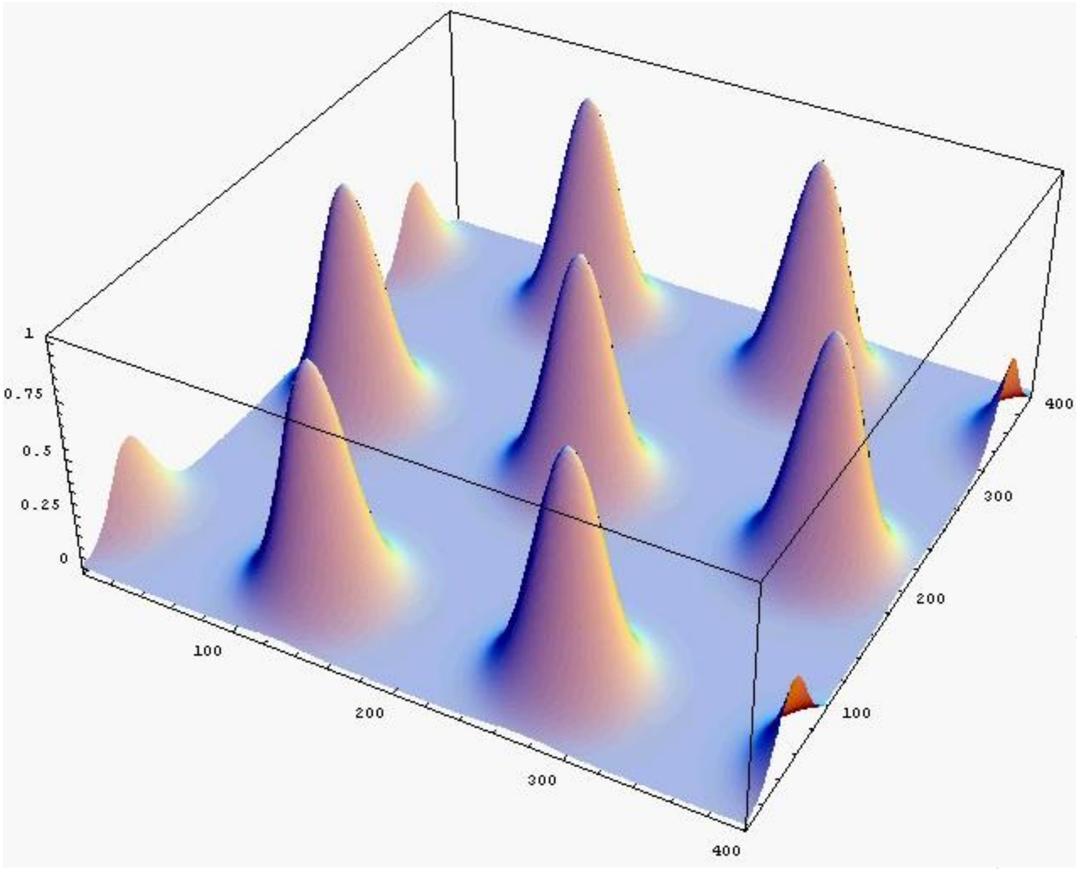
if $s > 5\lambda_n(\mathbf{B})$, and $\mathbf{X} \sim \rho_s(\mathbf{x}) = (1/s)^n e^{-\pi\|\mathbf{x}\|^2/s^2}$, then

$$\Delta(\mathbf{X} \bmod \mathbf{B}, \text{Uniform}(\mathbf{B})) < n2^{-110}$$

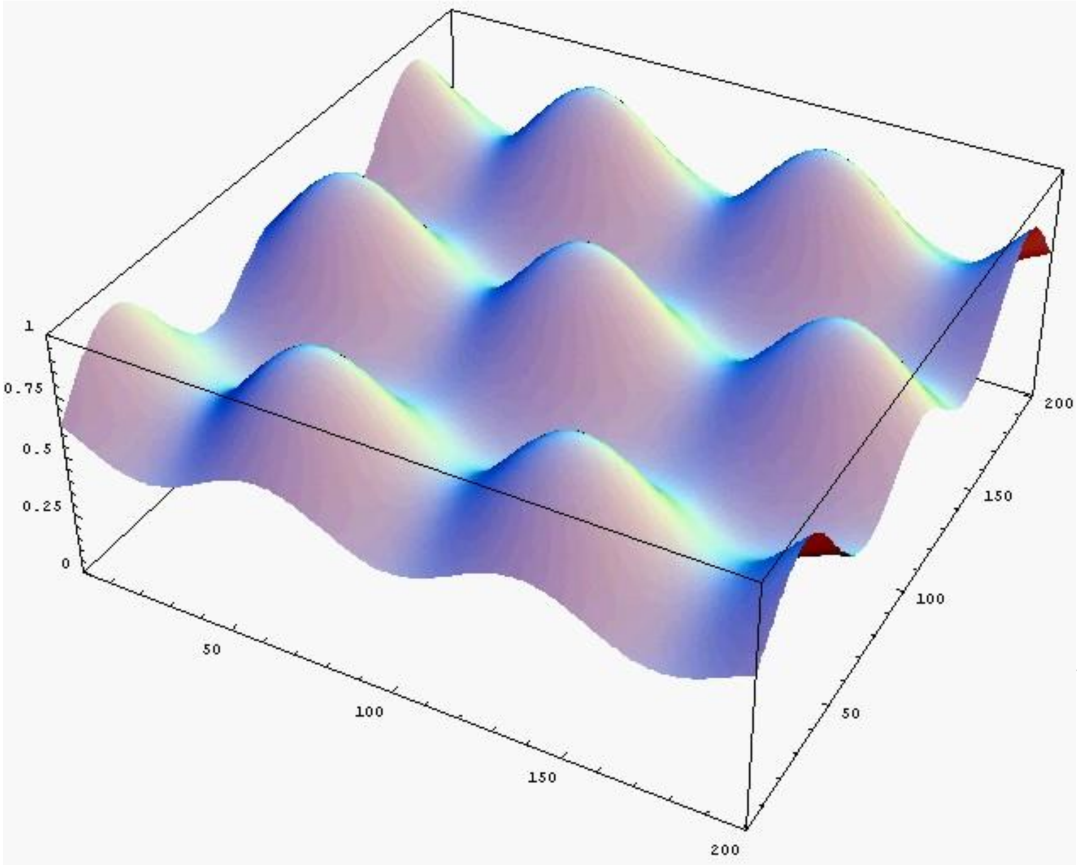
Gaussians on Lattice Points



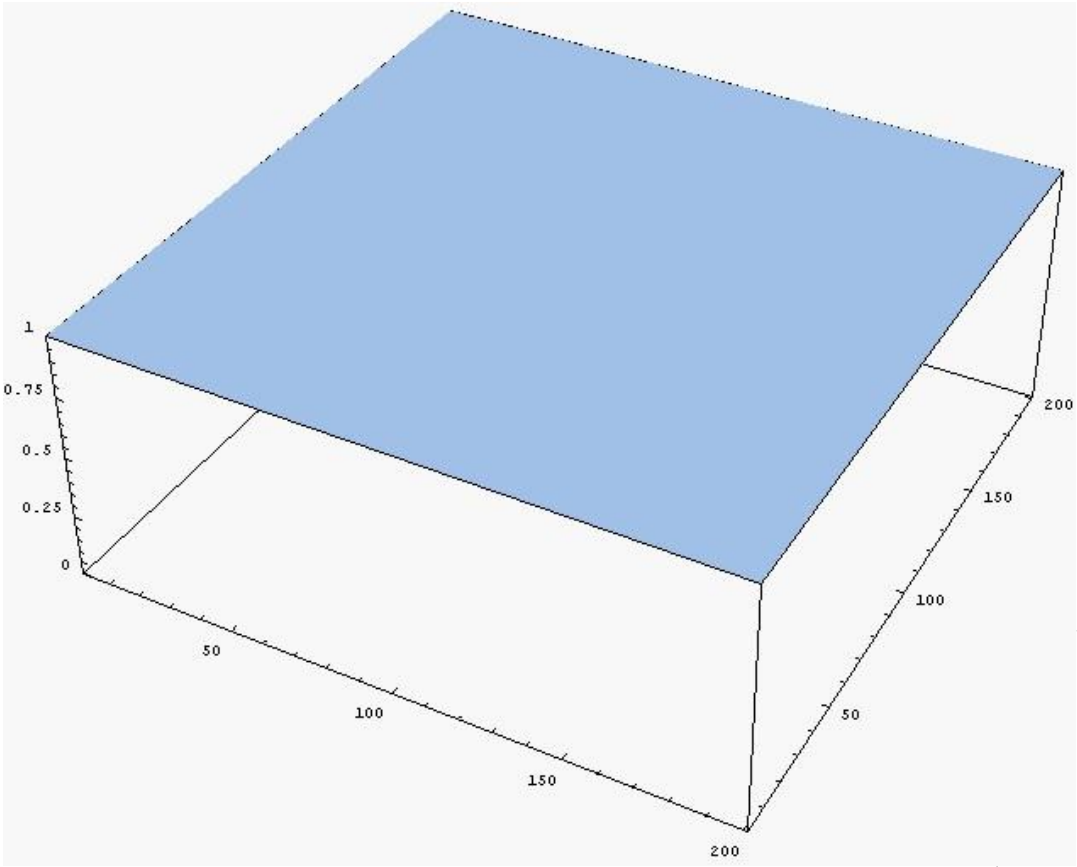
Gaussians on Lattice Points



Gaussians on Lattice Points



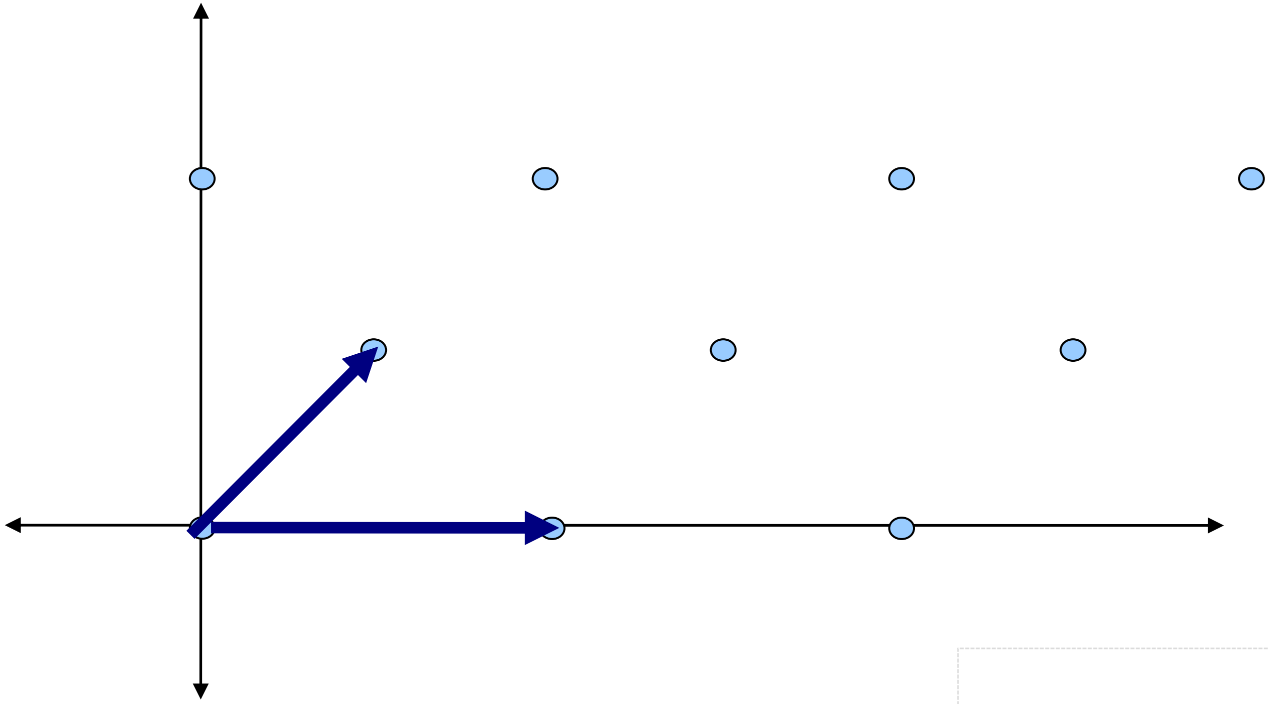
Gaussians on Lattice Points



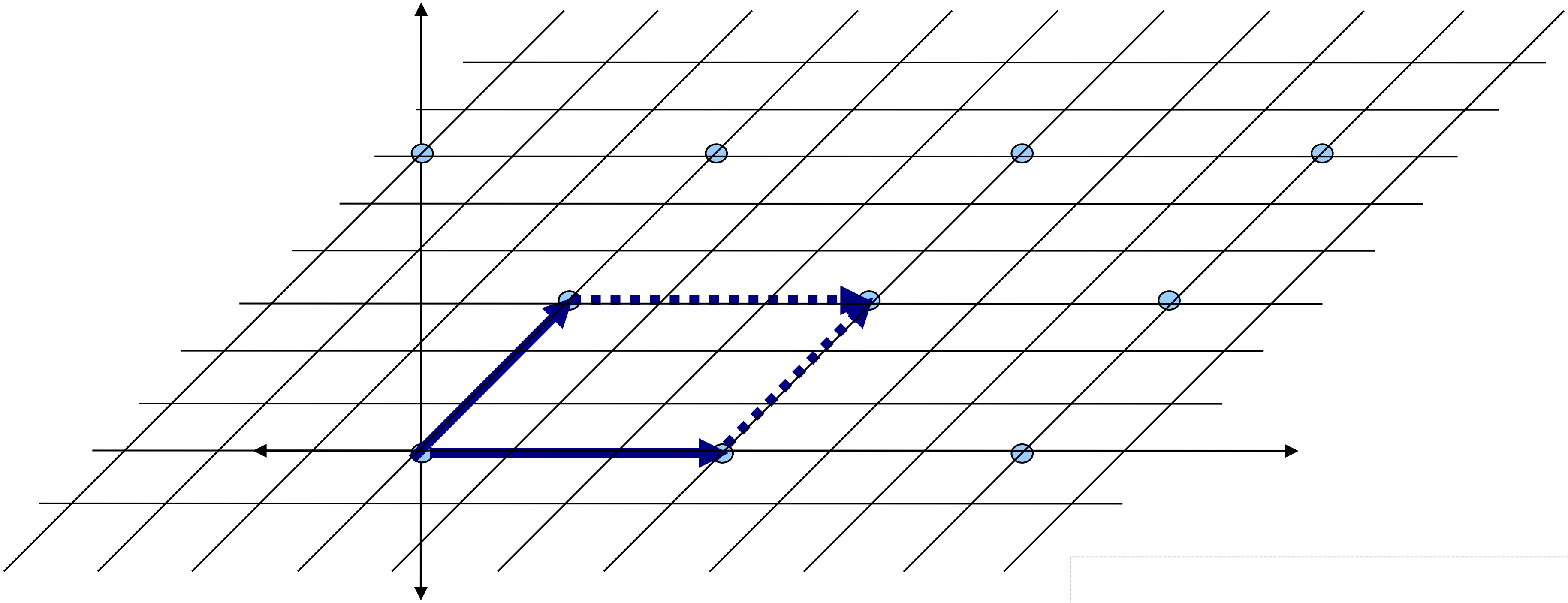
THE REDUCTION

[Ajtai ‘96, Micciancio and Regev ‘04]

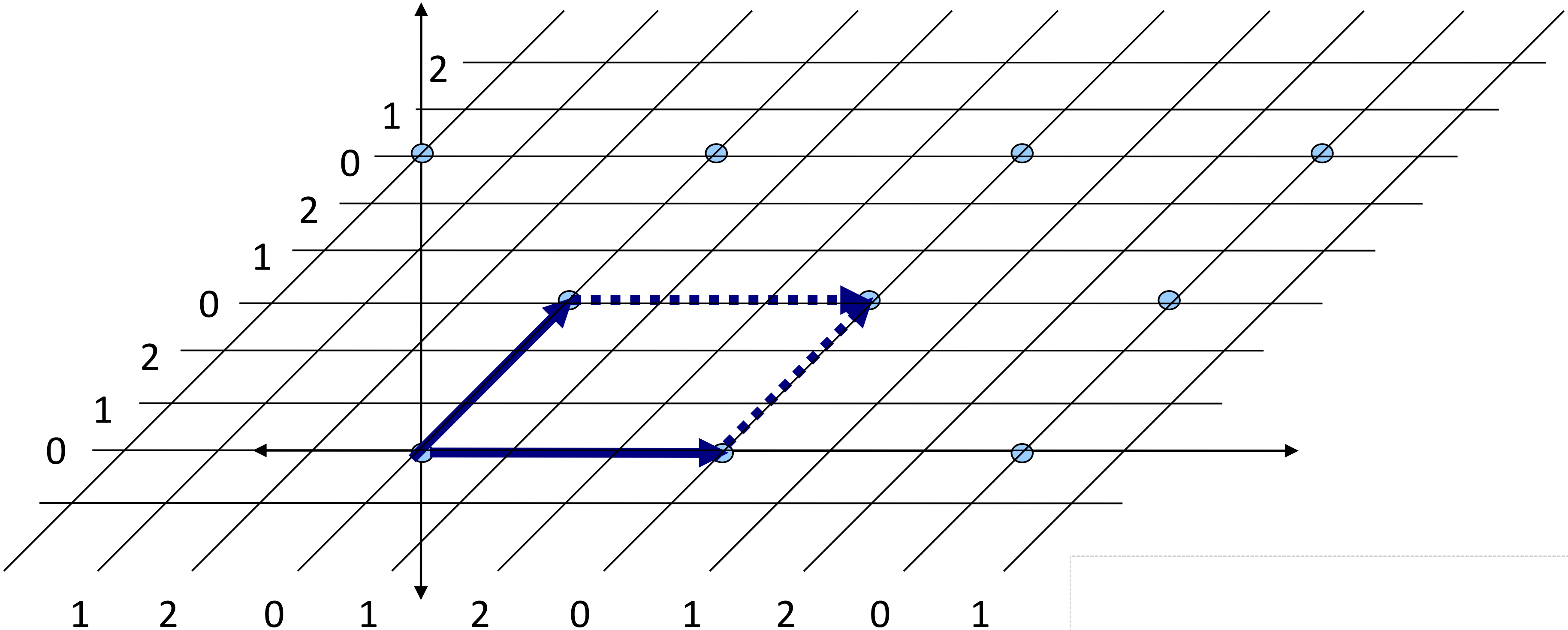
Worst-Case to Average-Case Reduction



Worst-Case to Average-Case Reduction



Worst-Case to Average-Case Reduction

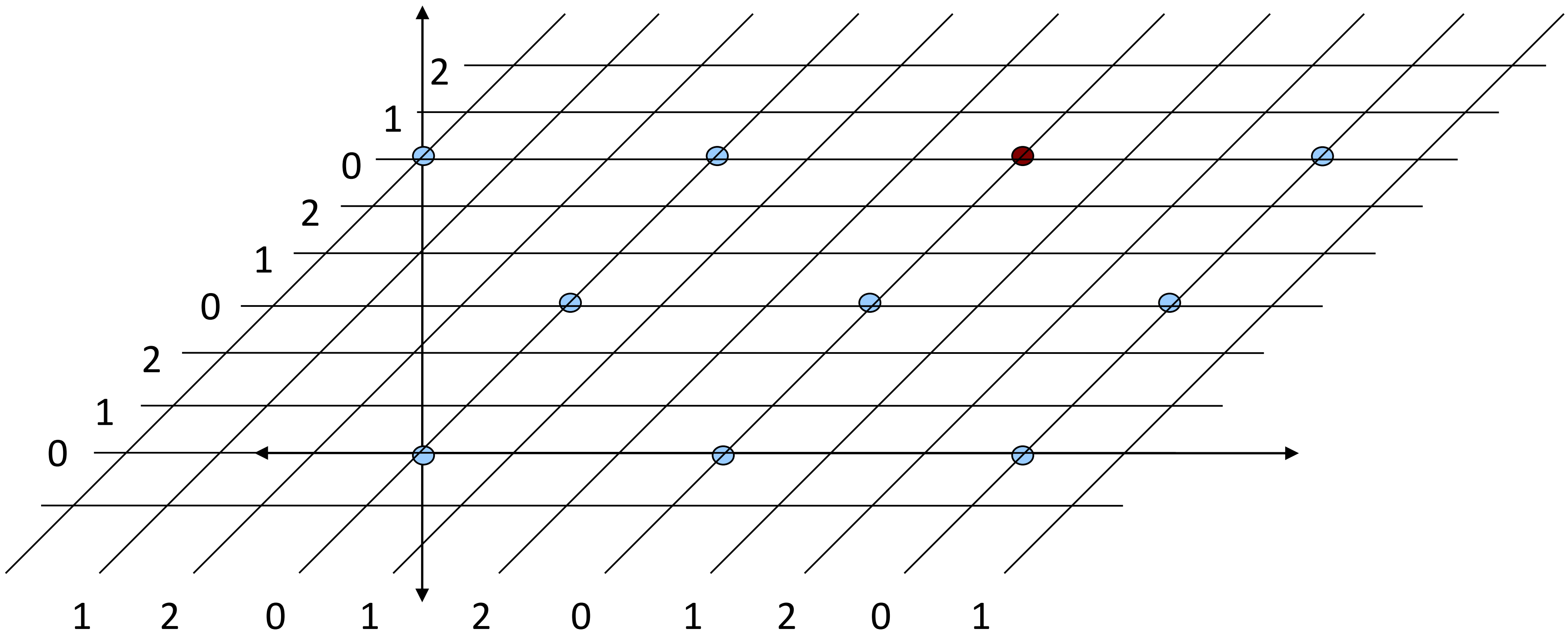


Important: All lattice points have label (0,0)

and

All points labeled (0,0) are lattice points

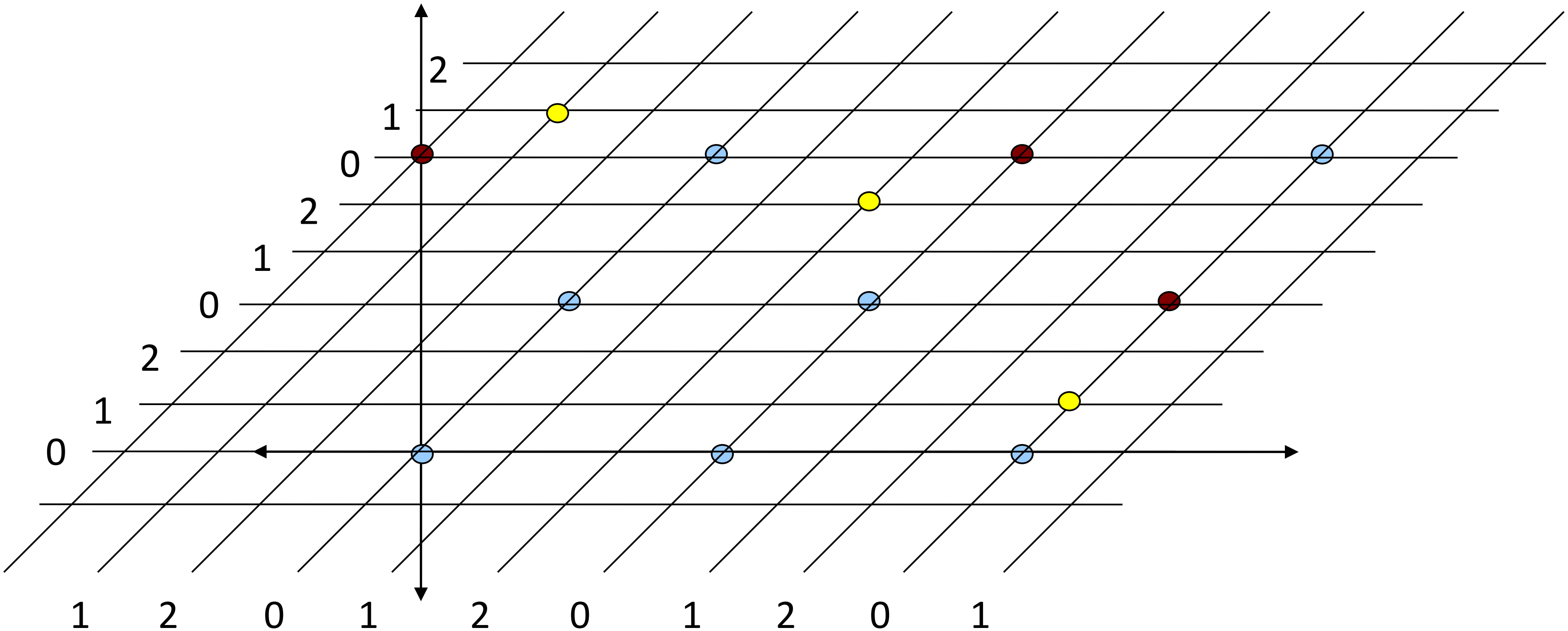
(**$\mathbf{0}^n$** in n dimensional lattices)



How to use the SIS oracle to find a short vector in any lattice:

Repeat m times:

Pick a random lattice point



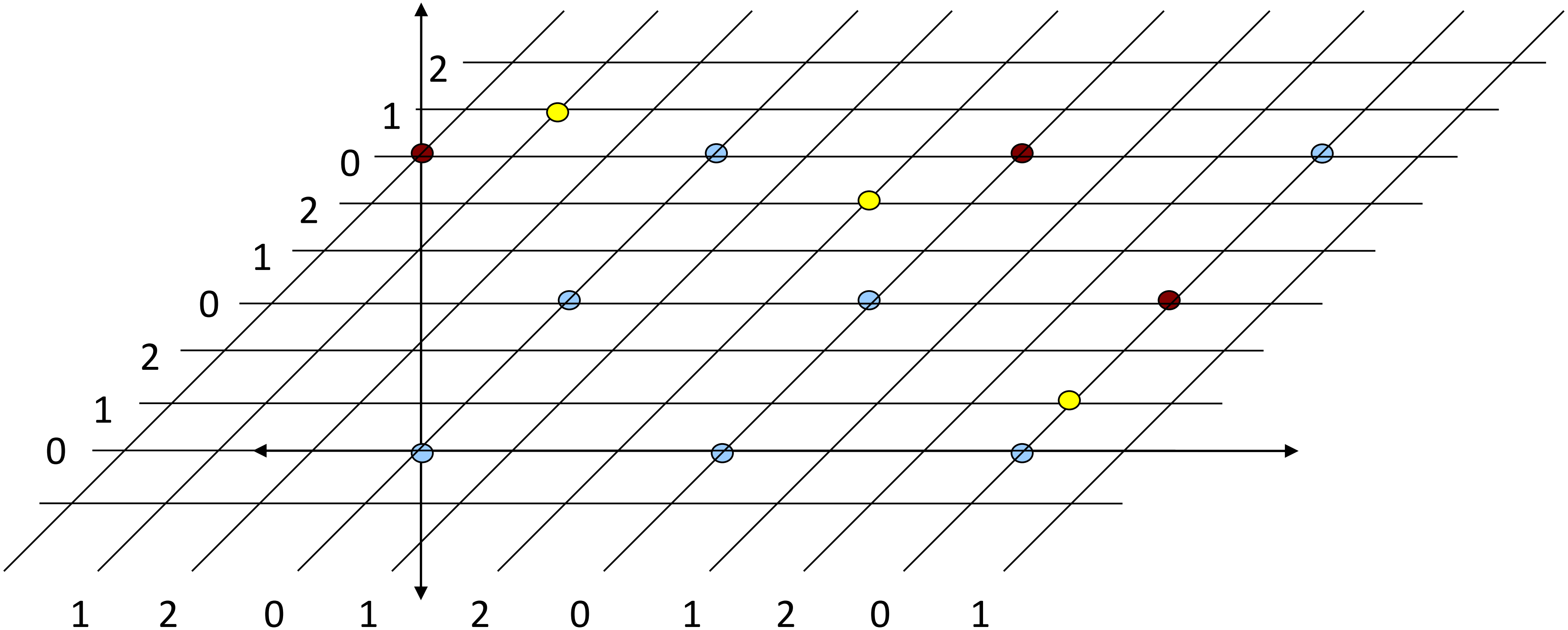
How to use the SIS oracle to find a short vector in any lattice:

Repeat m times:

Pick a random lattice point

Gaussian sample a point around the lattice point

All the samples are uniform in $\mathbf{Z}_q^n$



How to use the SIS oracle to find a short vector in any lattice:

Repeat m times:

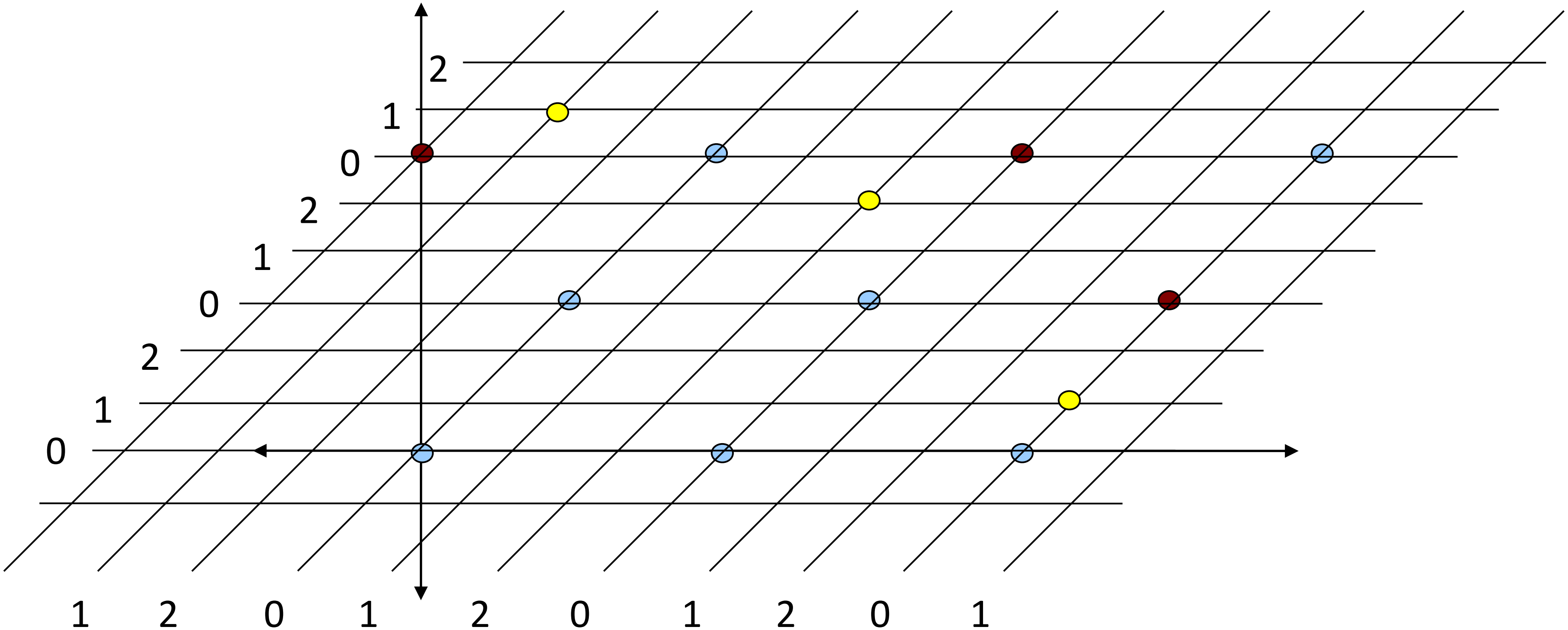
Pick a random lattice point

Gaussian sample a point around the lattice point

Give the m "$\mathbf{Z}_q^n$ samples" $\mathbf{a}_1,\ldots,\mathbf{a}_m$ to the SIS oracle

Oracle outputs $z_1,\ldots,z_m$ in {-1,0,1} such that:

$$\mathbf{a}_1 z_1 + \ldots + \mathbf{a}_m z_m = \mathbf{0}$$



Give the m "$\mathbf{Z}_q^n$ samples" $\mathbf{a}_1,\ldots,\mathbf{a}_m$ to the SIS oracle

Get $z_1,\ldots,z_m$ in $\{-1,0,1\}$ such that $\mathbf{a}_1 z_1 + \ldots + \mathbf{a}_m z_m = \mathbf{0}$

= $\mathbf{v}_i$

= $\mathbf{s}_i$

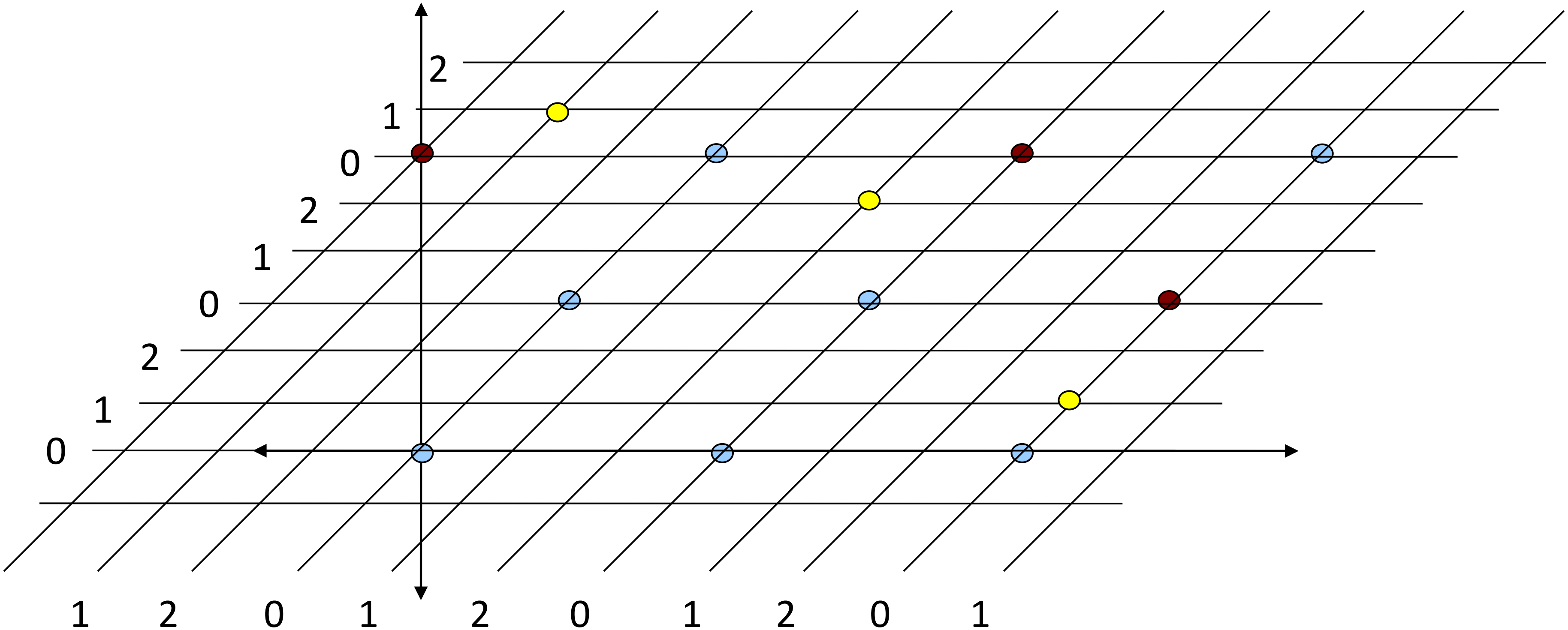
$\mathbf{v}_i + \mathbf{r}_i = \mathbf{s}_i$

$\mathbf{s}_1 z_1 + \ldots + \mathbf{s}_m z_m$ is a lattice vector, so

$(\mathbf{v}_1+\mathbf{r}_1)z_1 + \ldots + (\mathbf{v}_m+\mathbf{r}_m)z_m$ is too

$(\mathbf{v}_1\mathbf{z}_1+\ldots+\mathbf{v}_m\mathbf{z}_m) + (\mathbf{r}_1\mathbf{z}_1+\ldots+\mathbf{r}_m\mathbf{z}_m)$ is too

So, $\mathbf{r}_1\mathbf{z}_1+\ldots+\mathbf{r}_m\mathbf{z}_m$ is also lattice vector



Give the m "$\mathbf{Z}_q^n$ samples" $\mathbf{a}_1,\ldots,\mathbf{a}_m$ to the SIS oracle

Get $z_1,\ldots,z_m$ in {-1,0,1} such that $\mathbf{a}_1 z_1 + \ldots + \mathbf{a}_m z_m = \mathbf{0}$

● = $\mathbf{v}_i$

● = $\mathbf{s}_i$

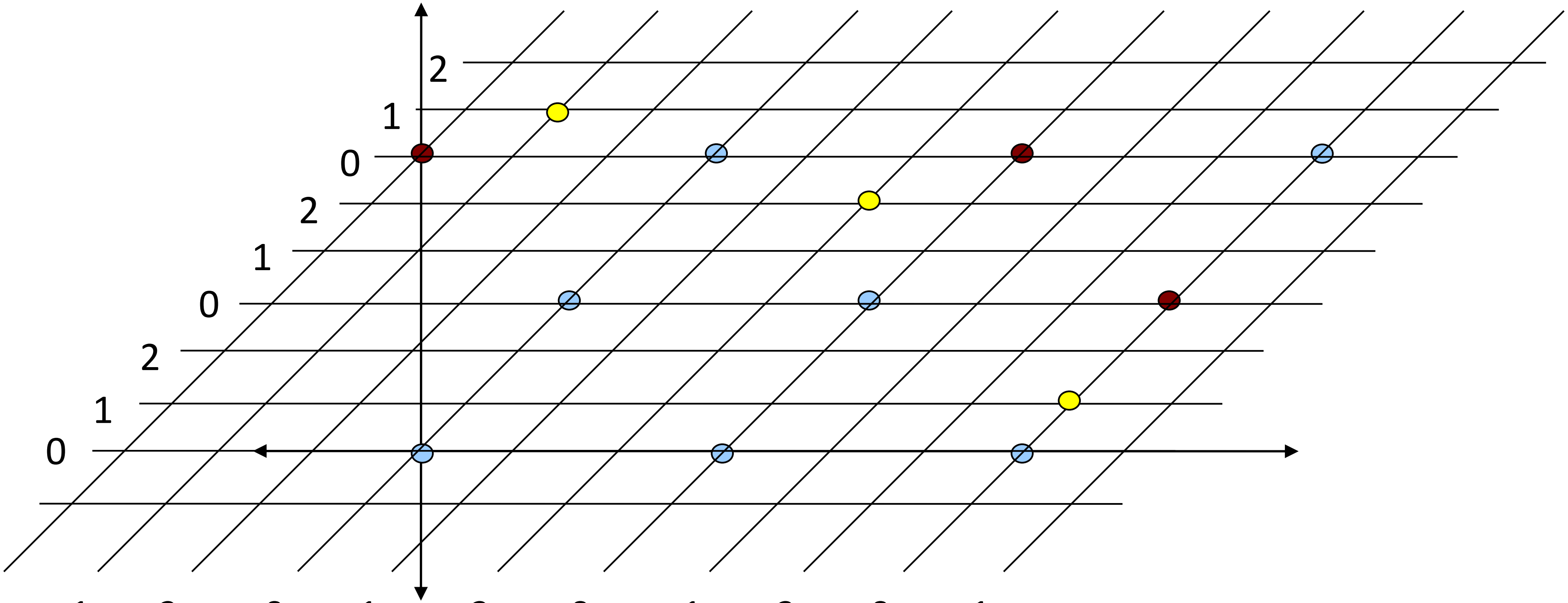
$\mathbf{v}_i + \mathbf{r}_i = \mathbf{s}_i$

So, $\mathbf{r}_1 z_1 + \ldots + \mathbf{r}_m z_m$ is also lattice vector

$\mathbf{r}_i$ are short vectors, z_i are in {-1,0,1}

So $\mathbf{r}_1 z_1 + \ldots + \mathbf{r}_m z_m$ is a **short** lattice vector

$\|\mathbf{r}_1 z_1 + \ldots + \mathbf{r}_m z_m\| \approx \tilde{O}(\sqrt{m})\|\mathbf{r}_i\|$



Give the m "$\mathbf{Z}_\mathbf{q}^\mathbf{n}$ samples" $\mathbf{a_1},\ldots,\mathbf{a_m}$ to the SIS oracle

Get $z_1,\ldots,z_m$ in {-1,0,1} such that $\mathbf{a_1}z_1 + \ldots + \mathbf{a_m}z_m = \mathbf{0}$

 $= \mathbf{v_i}$

 $= \mathbf{s_i}$

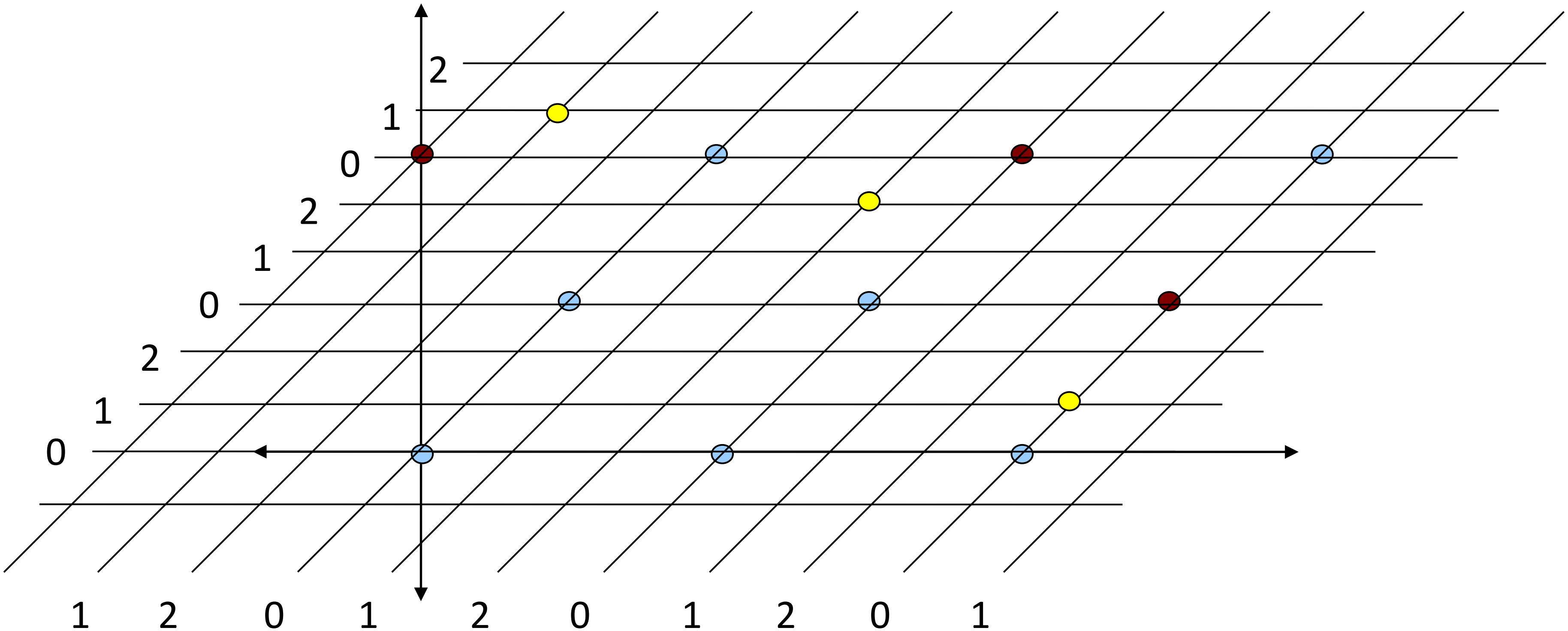
$\mathbf{v_i} + \mathbf{r_i} = \mathbf{s_i}$

$||\mathbf{r_1}z_1+\ldots+\mathbf{r_m}z_m|| \approx \tilde{O}(\sqrt{m})||\mathbf{r_i}||$

Reduction works when

$\mathbf{r_i} \sim \rho_s(\mathbf{x}) = (1/s)^n e^{-\pi|\mathbf{x}|^2/s^2}$ for $s>5\lambda_n$

So $||\mathbf{r_i}|| \approx 5\lambda_n\sqrt{n}$



$||\mathbf{r_1}z_1+\ldots+\mathbf{r_m}z_m|| \approx \tilde{O}(\sqrt{m})||\mathbf{r_i}||$

$\approx \tilde{O}(\sqrt{mn})\ \lambda_n \approx \tilde{O}(n)\ \lambda_n$

Can either guess λ_n using binary search or keep using s=length of the largest vector/$\tilde{O}(n)$ to find a shorter vector, and this should keep working until the length of the largest vector < $\tilde{O}(n)\ \lambda_{n,}$ which solves $\mathrm{SIVP}_{\tilde{O}(n)}$

Some Technicalities

- You can't sample a "uniformly random" lattice point
  - In the proofs we work with $\mathbf{R}^n$ / $\mathbf{L}$
- What if $\mathbf{r_1}z_1+\ldots+\mathbf{r_m}z_m$ is 0?
  - Can show that with non-negligible it is in fact linearly independent of the n-1 non-longest vectors.
  - This is because given an $\mathbf{s_i}$, there are many possible $\mathbf{r_i}$
- Gaussian Sampling doesn't give us points on the grid
  - Can round to a grid point
  - Need to be mindful to bound the extra "rounding distance"
  - Alternatively, sample the grid point directly (using an algorithm you will see tomorrow)