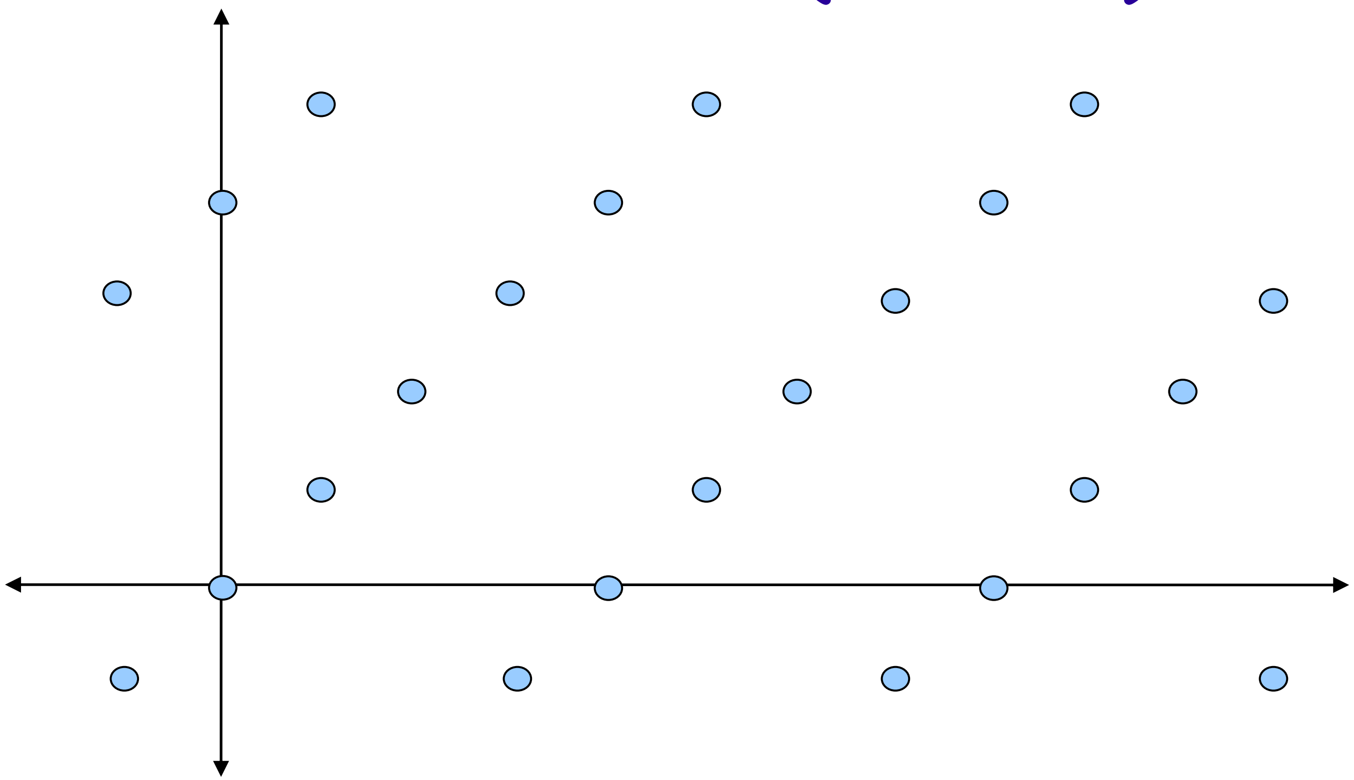
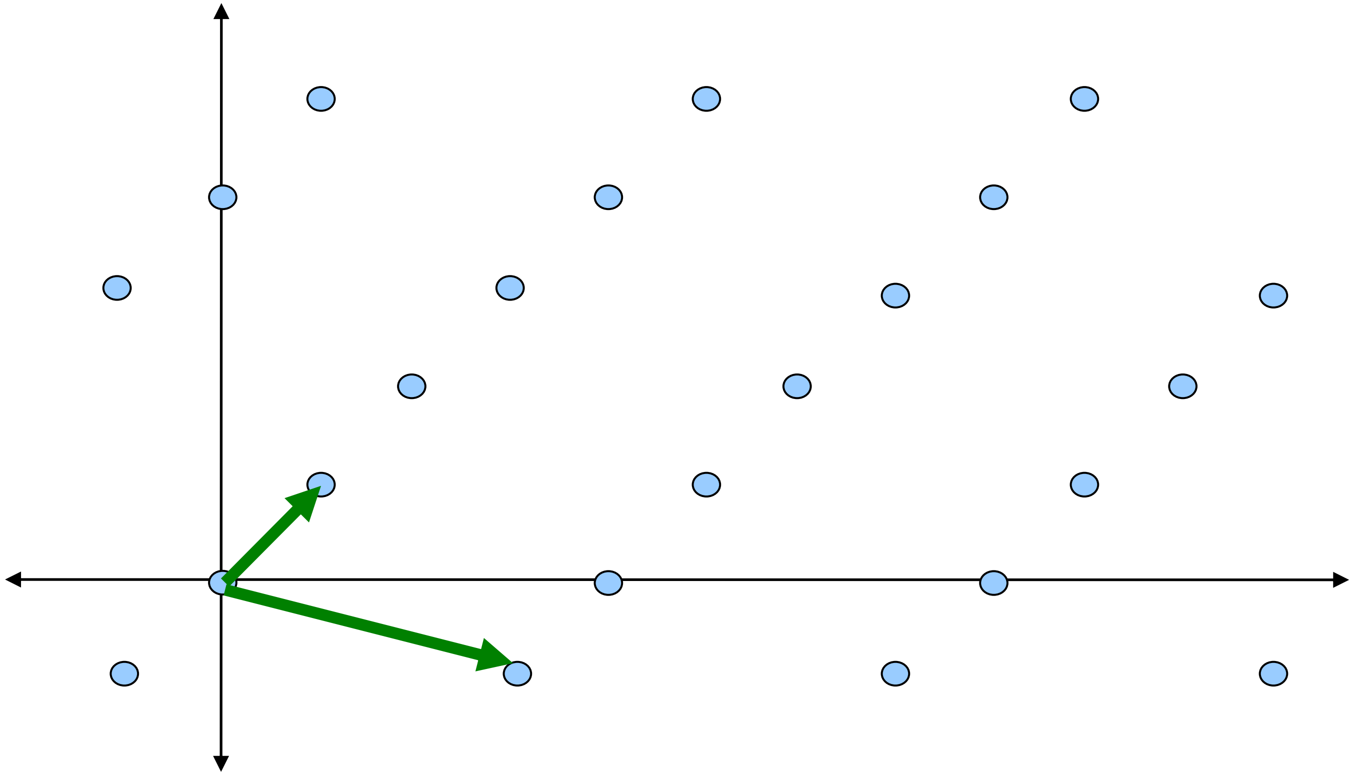
Shortest Independent Vector Problem (SIVP)



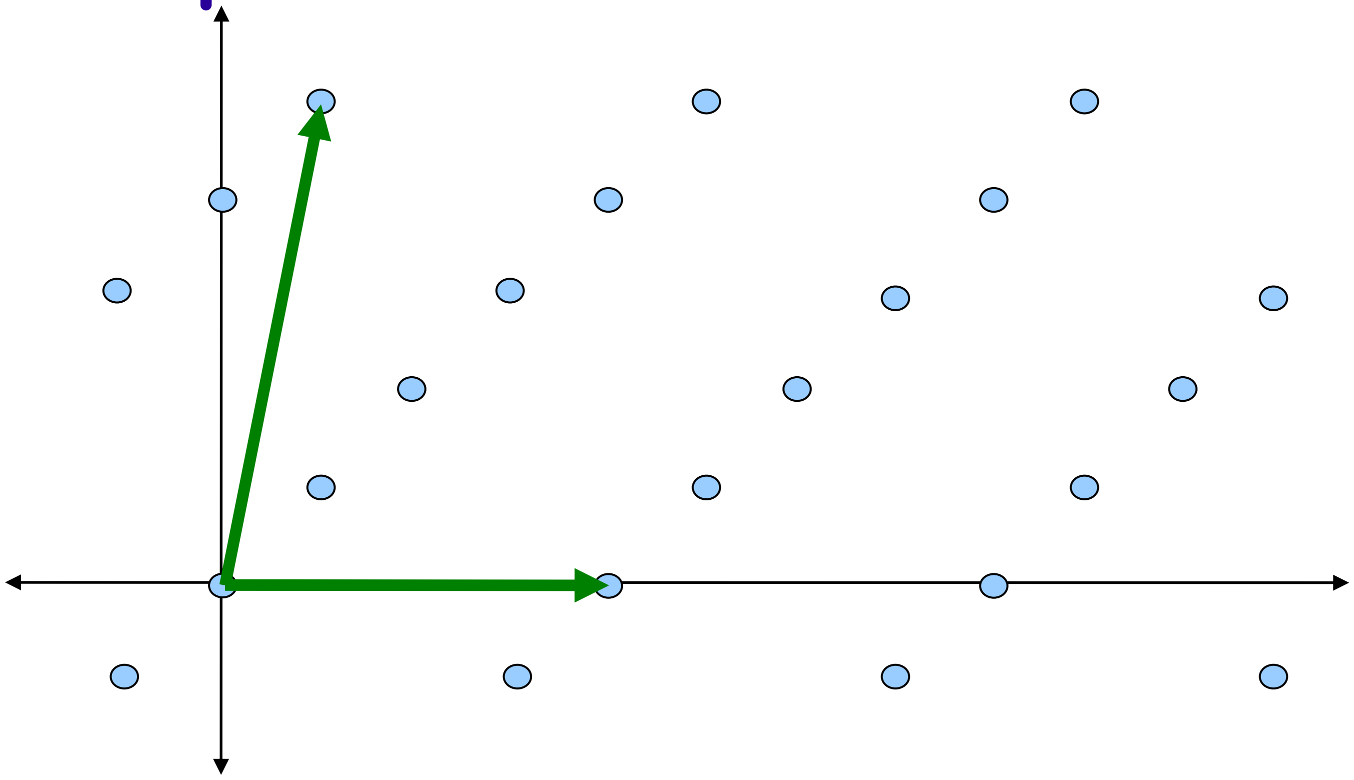
Find n short linearly independent vectors

Shortest Independent Vector Problem (SIVP)

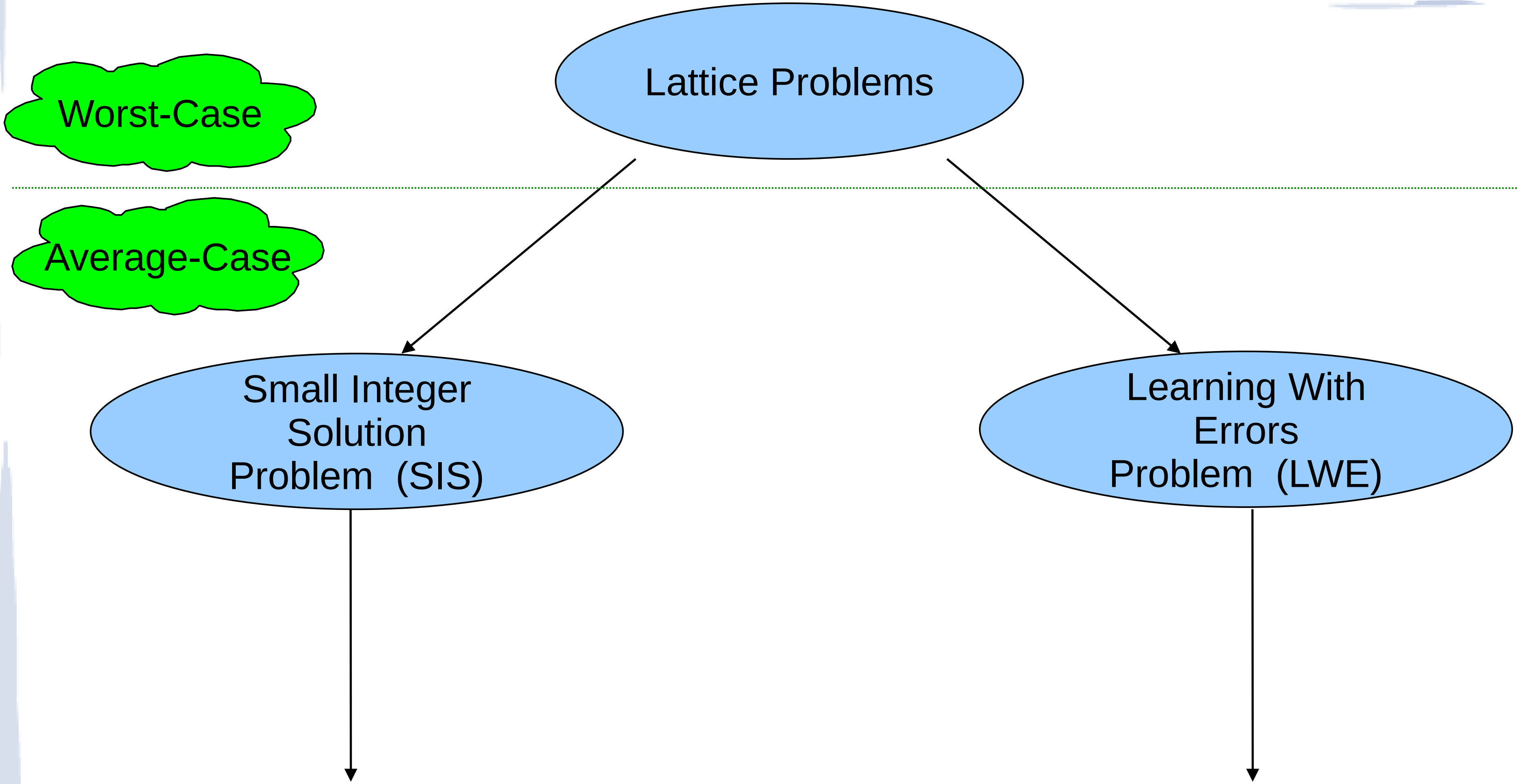


Find n short linearly independent vectors

Approximate Shortest Independent Vector Problem



Find n *pretty* short linearly independent vectors

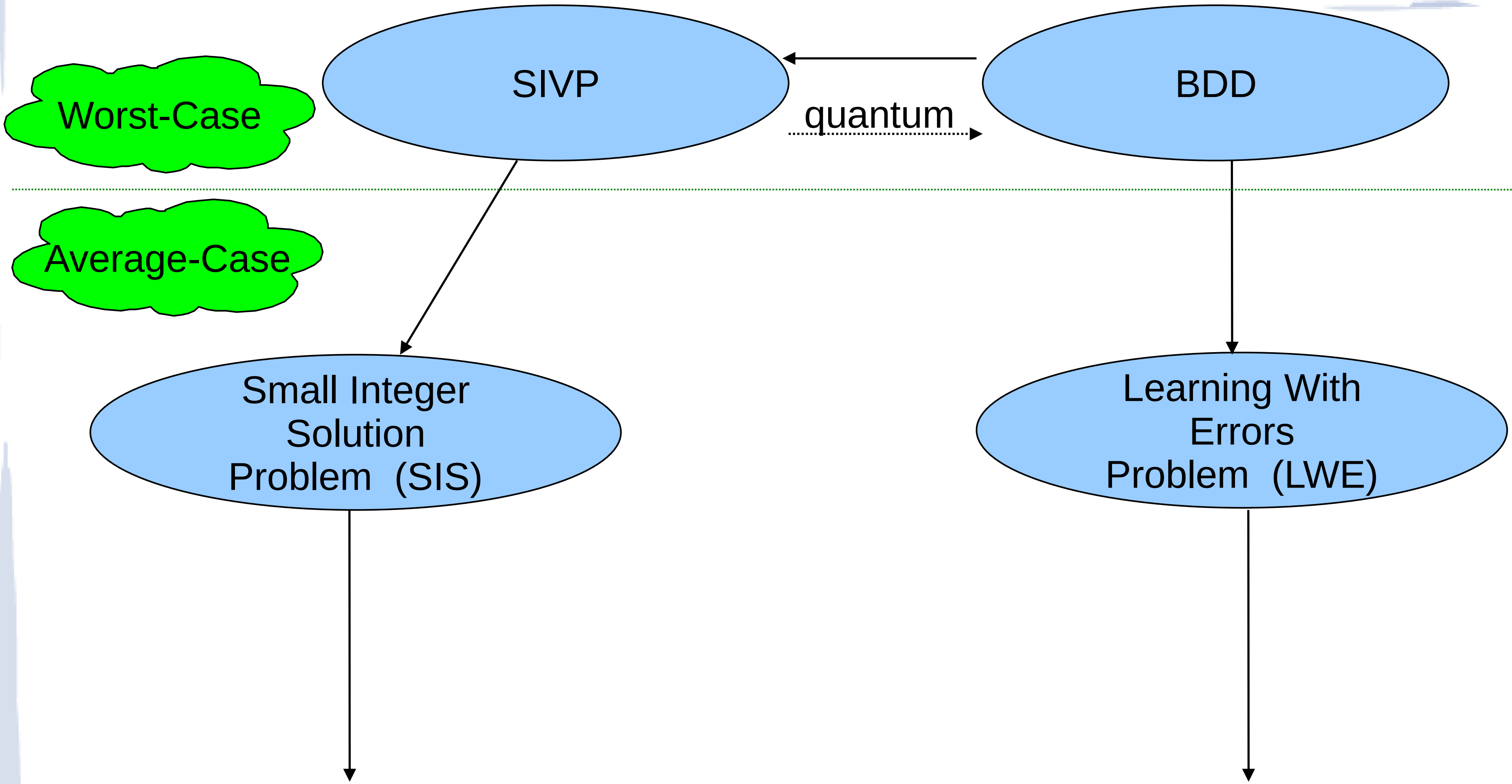


One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes

(Minicrypt)

Public Key Encryption
Oblivious Transfer
Identity-Based Encryption
Hierarchical Identity-Based Encryption

(Cryptomania)



One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes

(Minicrypt)

Public Key Encryption
Oblivious Transfer
Identity-Based Encryption
Hierarchical Identity-Based Encryption

(Cryptomania)

Small Integer Solution Problem

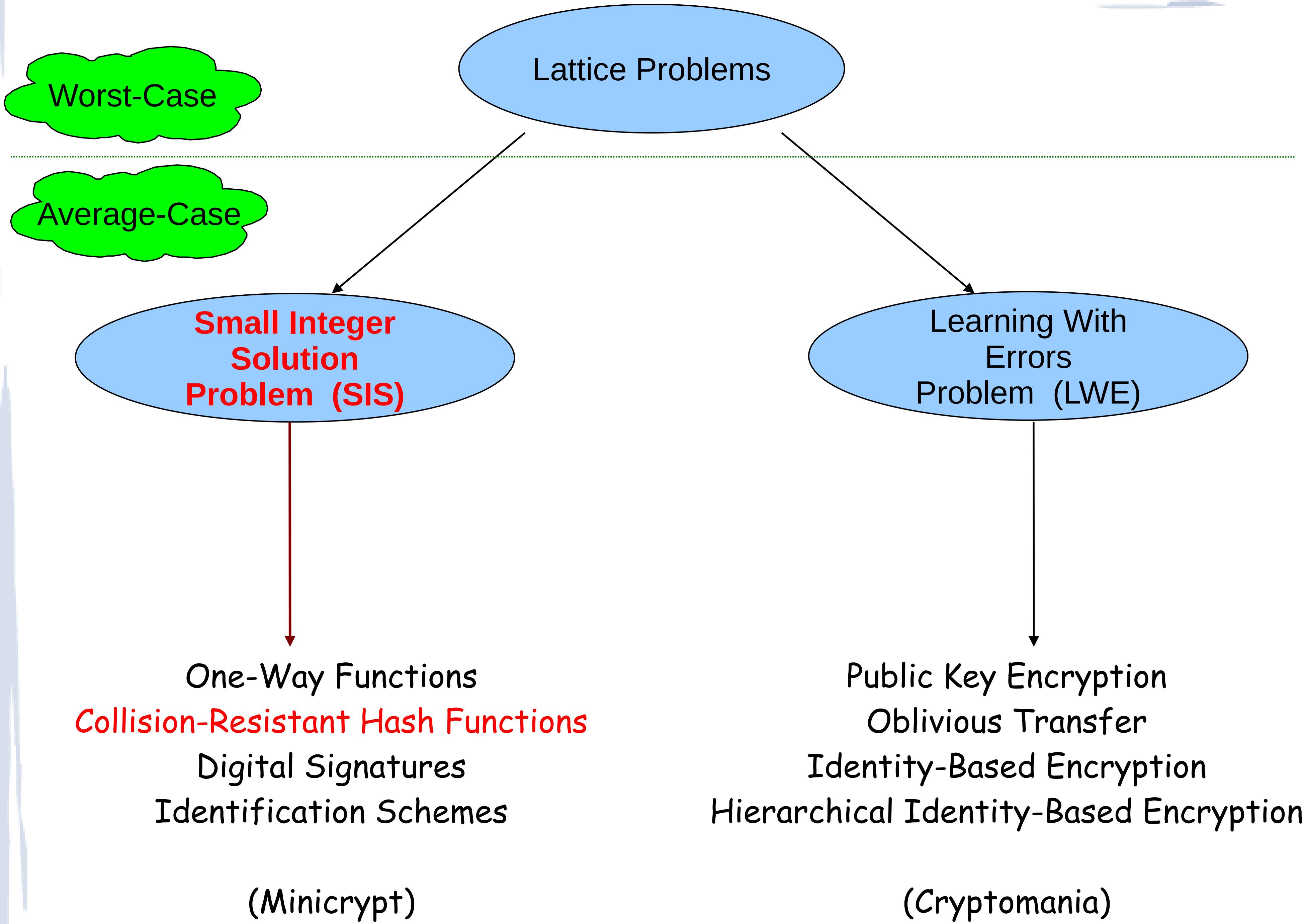
Given: Random vectors $a_1,\ldots,a_m$ in $\mathbf{Z}_q^n$

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

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

Observations:

- If size of z_i is not restricted, then the problem is trivial
- Immediately implies a collision-resistant hash function


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
Oblivious Transfer
Identity-Based Encryption
Hierarchical Identity-Based Encryption
(Cryptomania)

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:

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

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

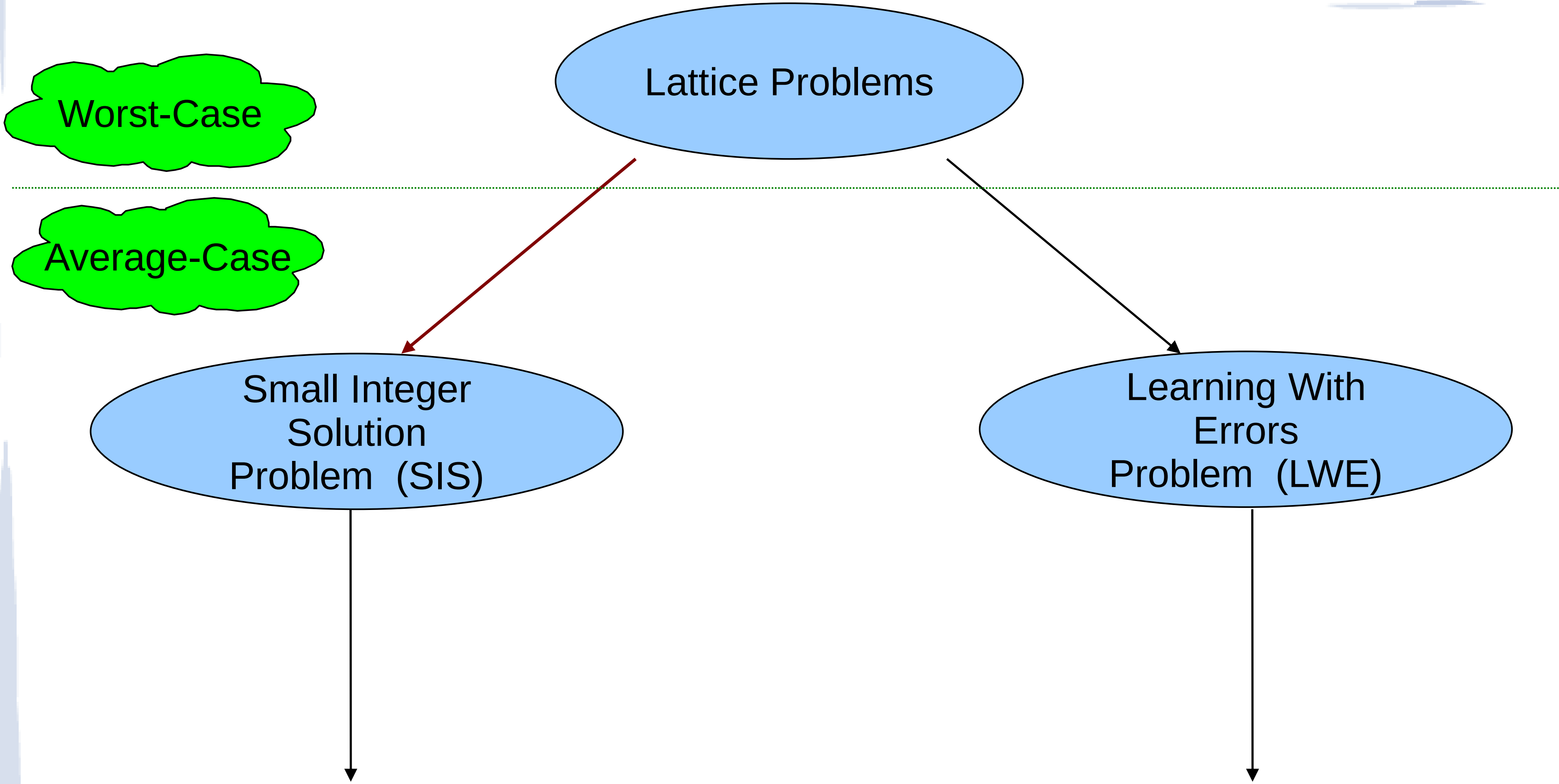
$h_A(z_1,\ldots,z_m)=a_1z_1 + \ldots + a_mz_m$

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

Set $m>n\log q$ to get compression

Collision: $a_1z_1 + \ldots + a_mz_m = a_1y_1 + \ldots + a_my_m$

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

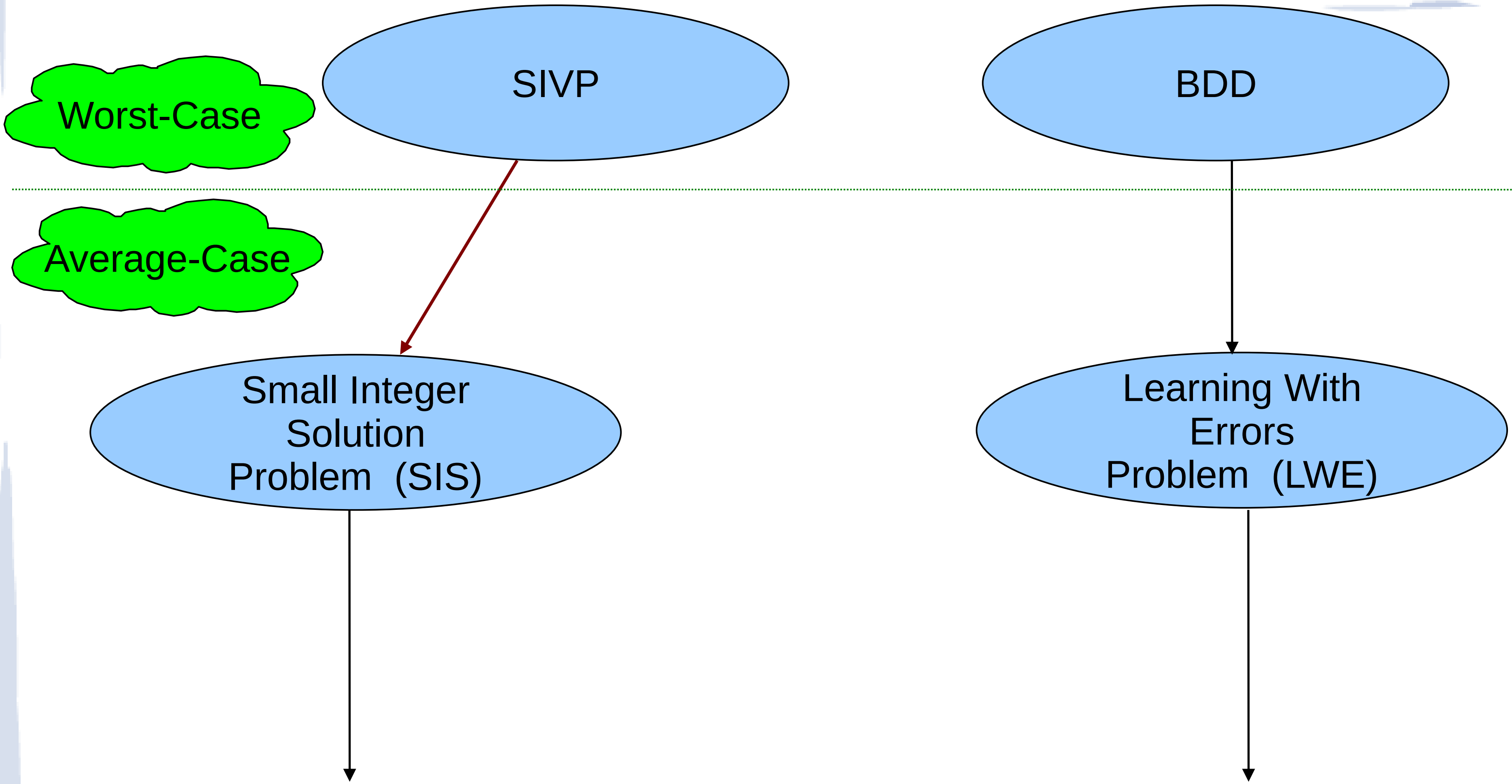


One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes

(Minicrypt)

Public Key Encryption
Oblivious Transfer
Identity-Based Encryption
Hierarchical Identity-Based Encryption

(Cryptomania)



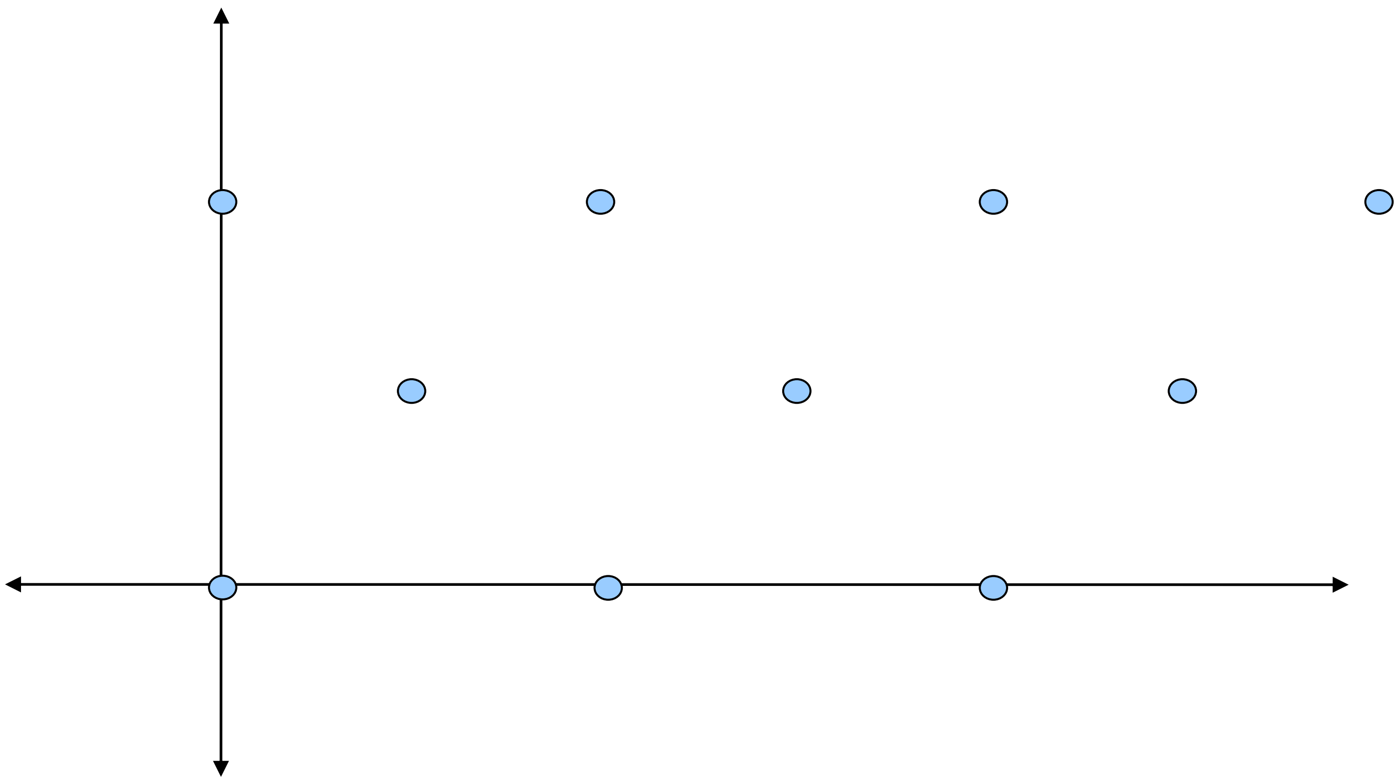
One-Way Functions
Collision-Resistant Hash Functions
Digital Signatures
Identification Schemes

(Minicrypt)

Public Key Encryption
Oblivious Transfer
Identity-Based Encryption
Hierarchical Identity-Based Encryption

(Cryptomania)

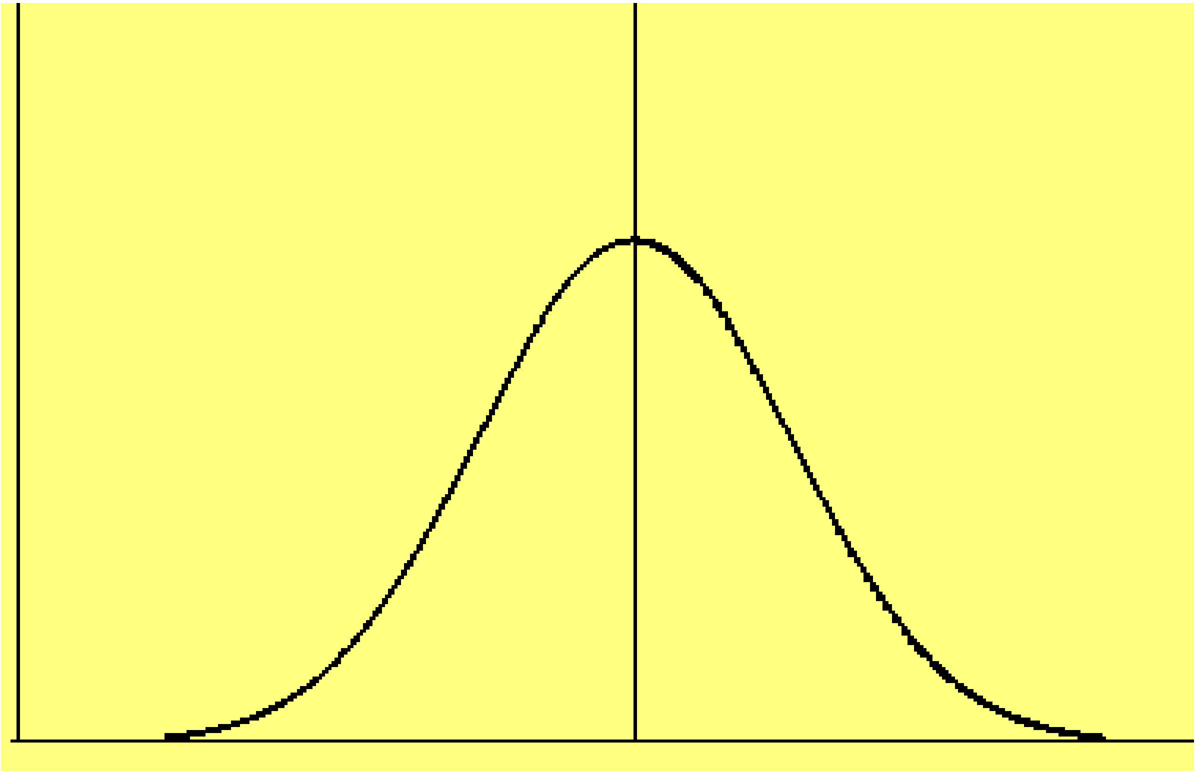
For Any Lattice ...



Consider the distribution obtained by:

1. Pick a uniformly random lattice point
2. Sample from a Gaussian distribution centered at the lattice point

One-Dimensional Gaussian Distribution



Two-Dimensional Gaussian Distribution

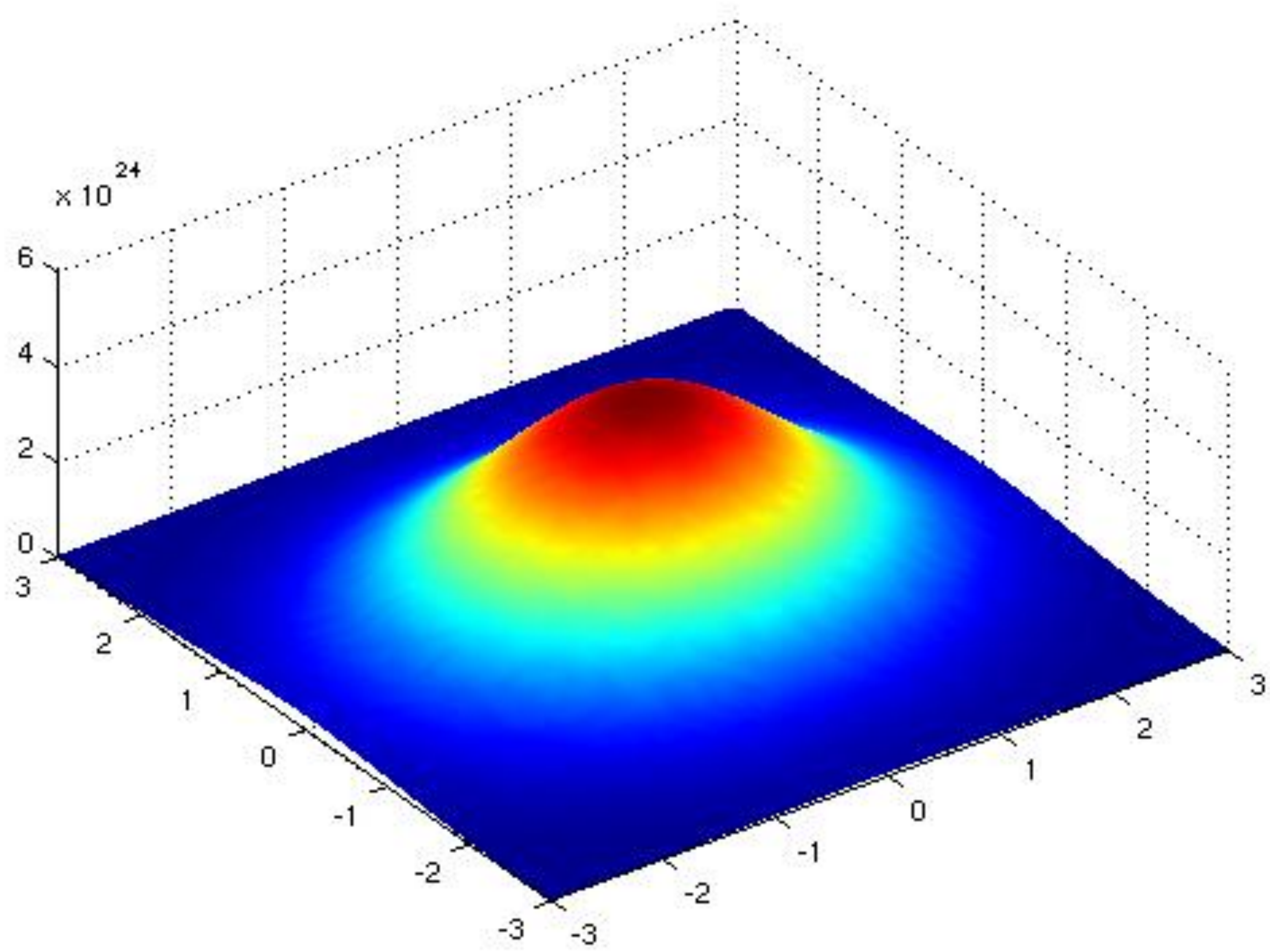


Image courtesy of wikipedia

Gaussians on Lattice Points

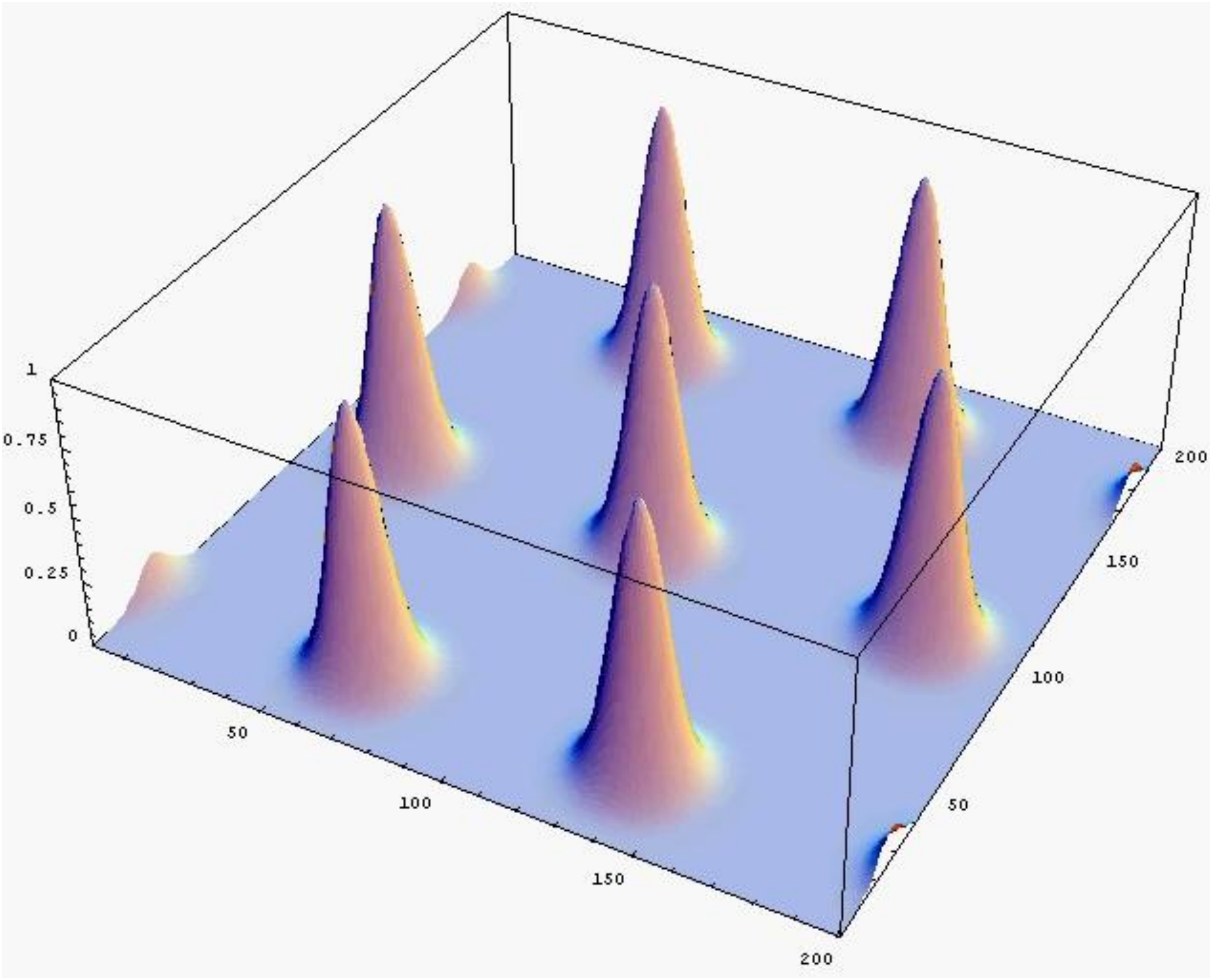


Image courtesy of Oded Regev

Gaussians on Lattice Points

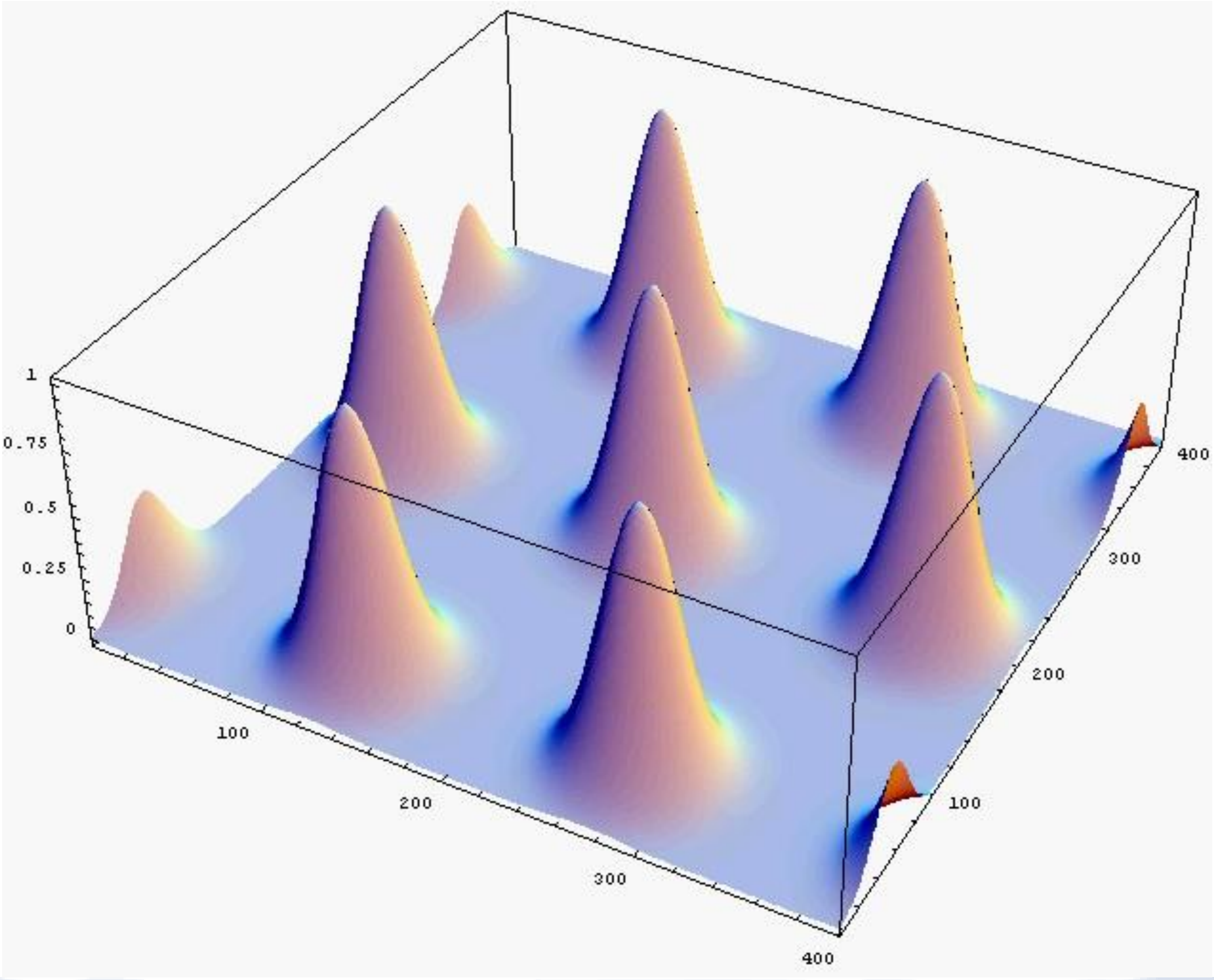


Image courtesy of Oded Regev

Gaussians on Lattice Points

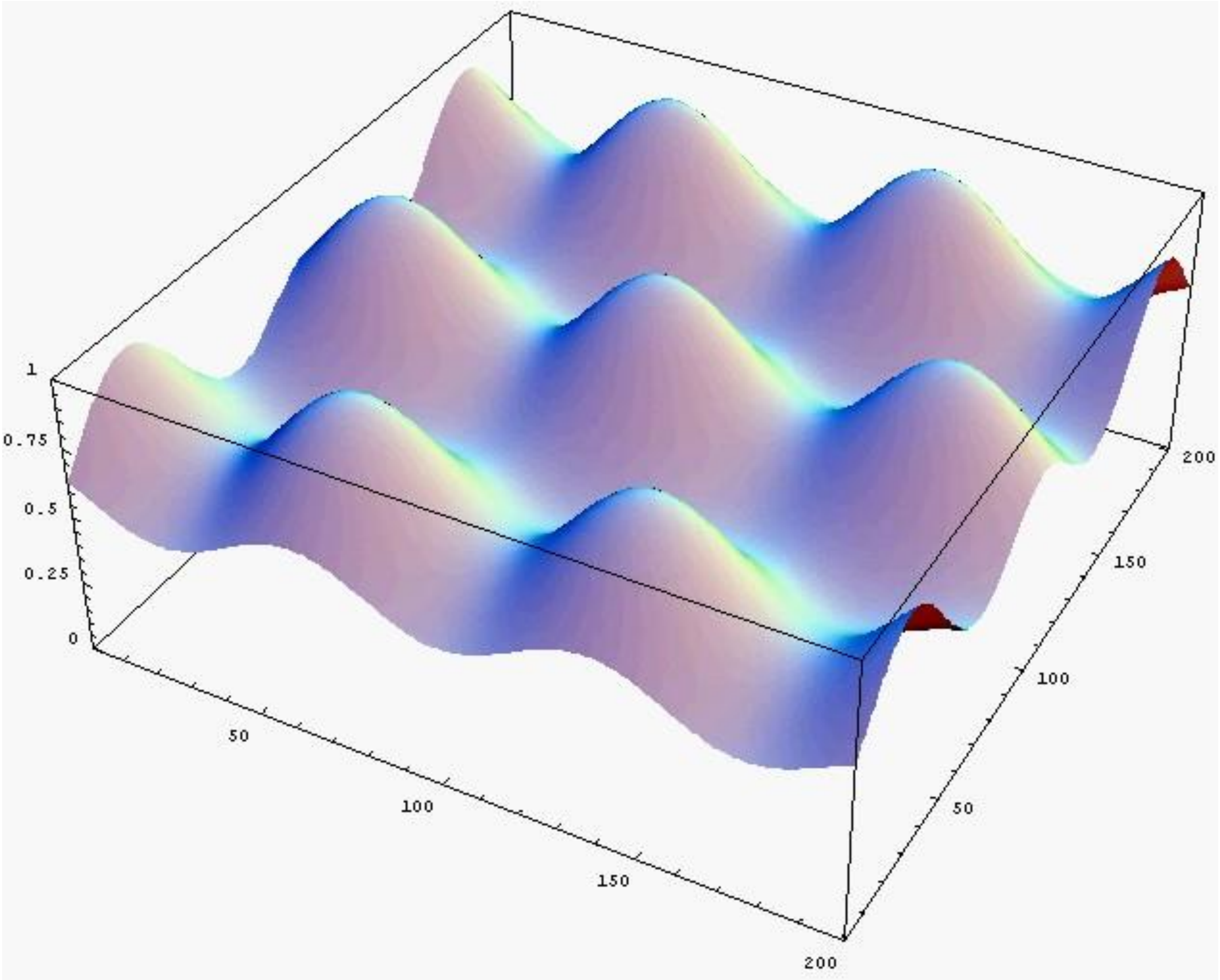


Image courtesy of Oded Regev

Gaussians on Lattice Points

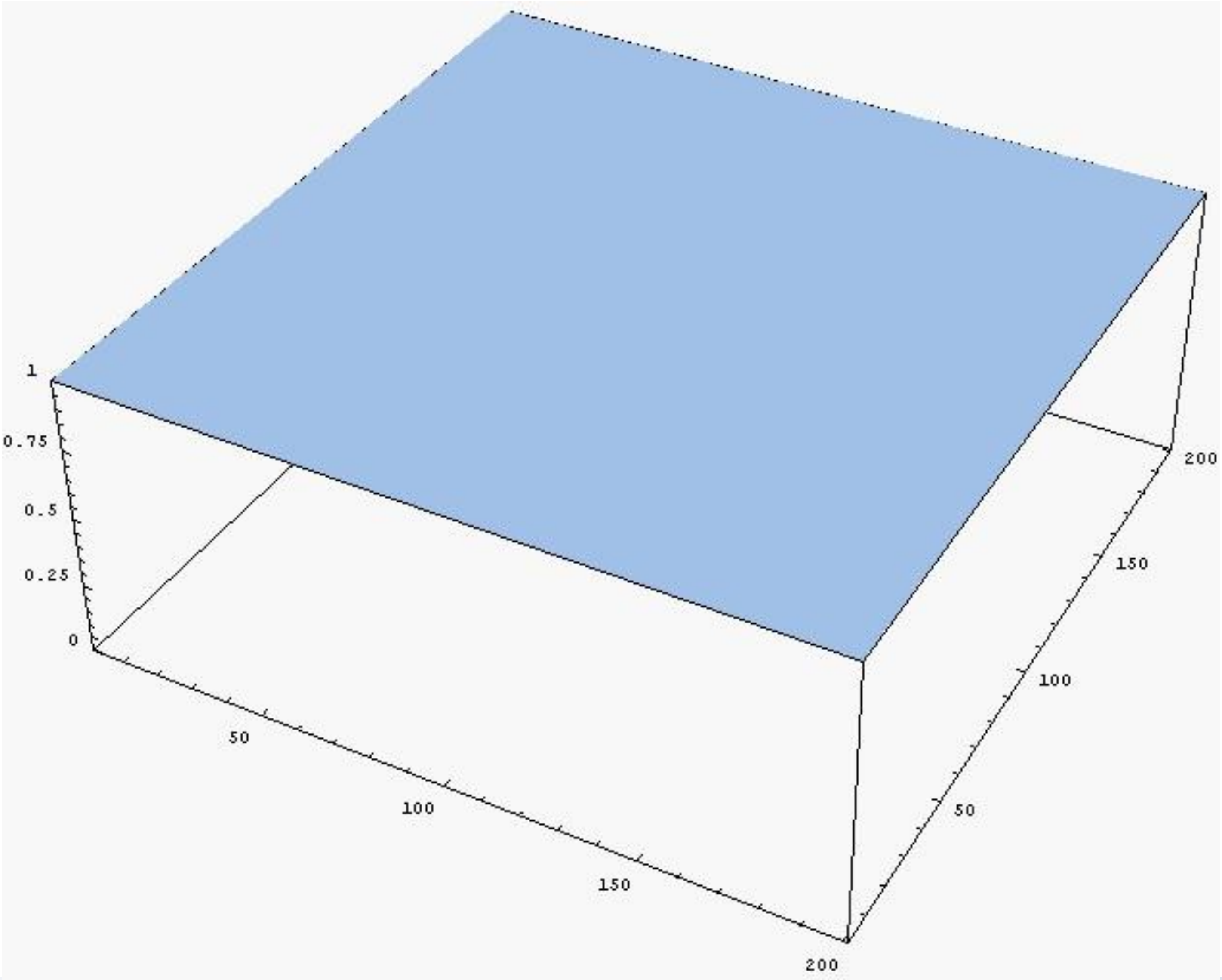
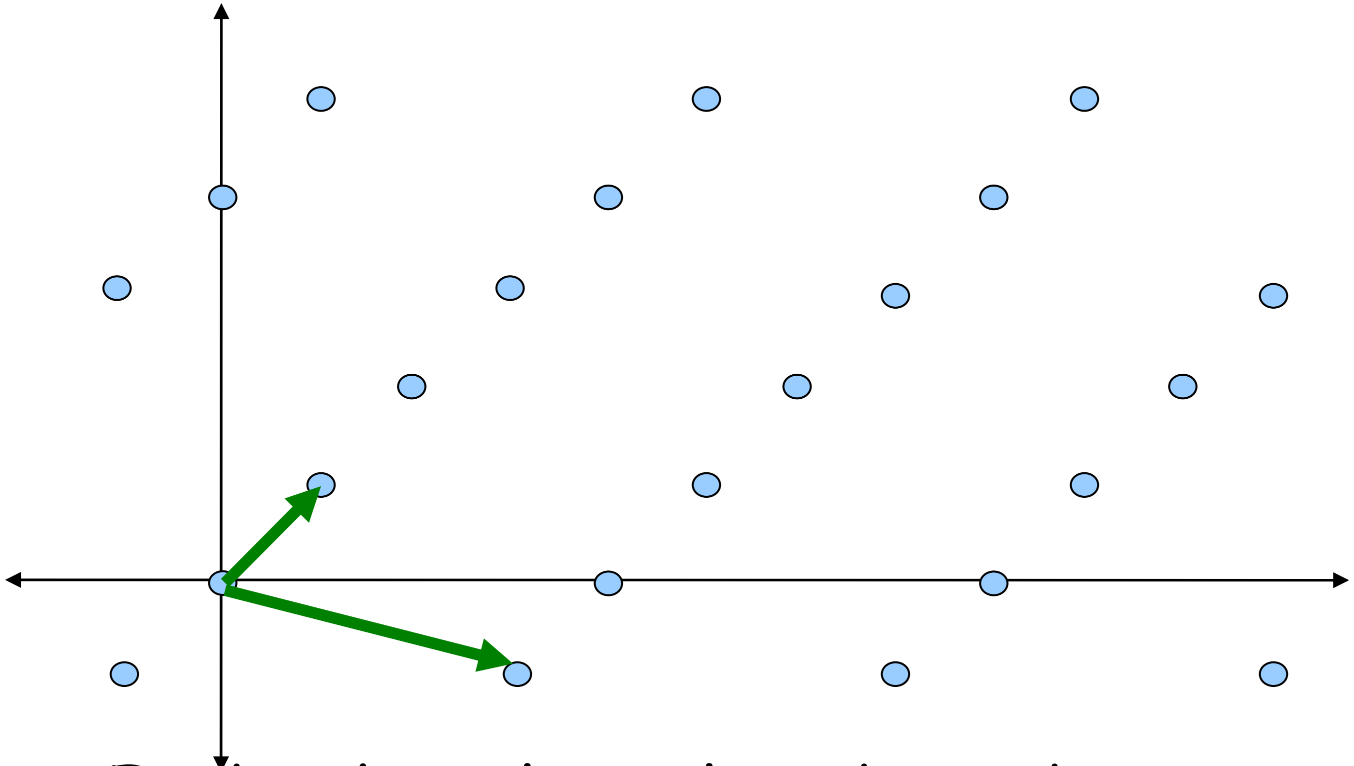


Image courtesy of Oded Regev

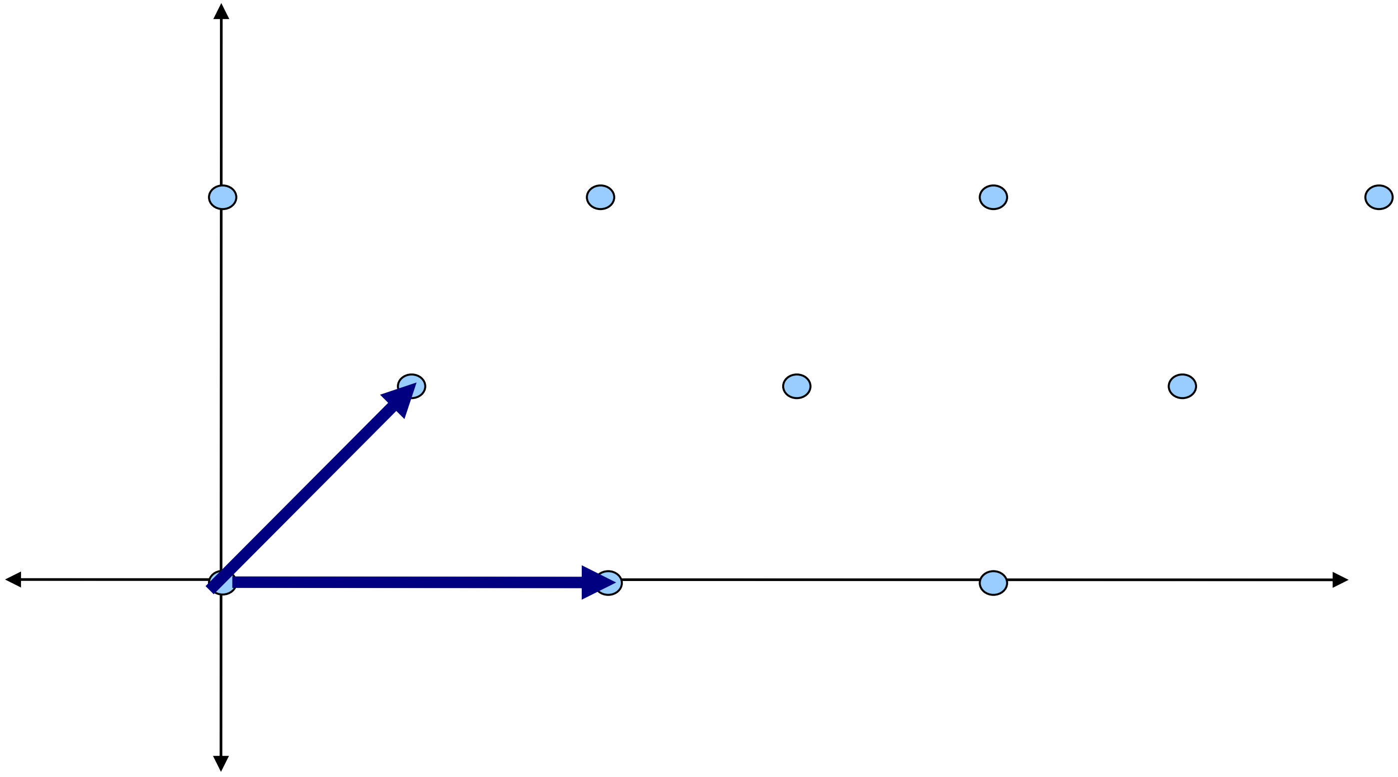
Shortest Independent Vector Problem (SIVP)



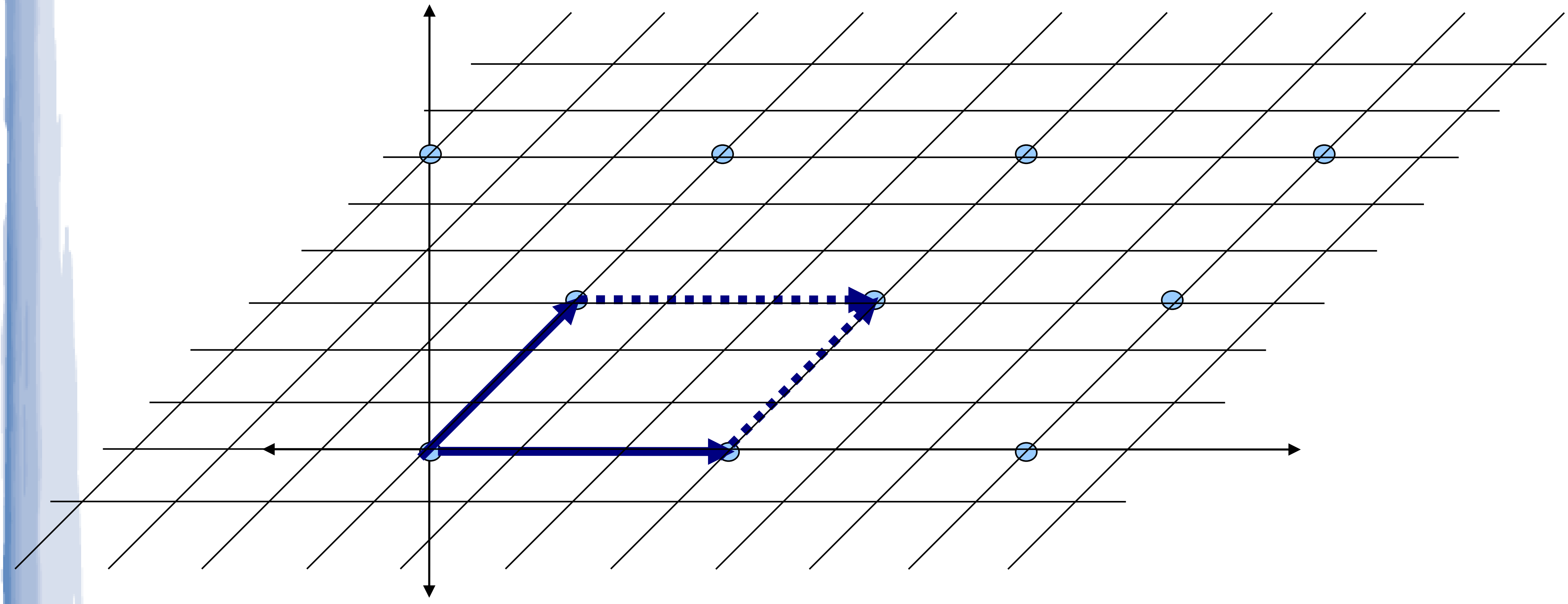
Find n short linearly independent vectors

Standard deviation of Gaussian that leads to the uniform distribution is related to the length of the longest vector in SIVP solution

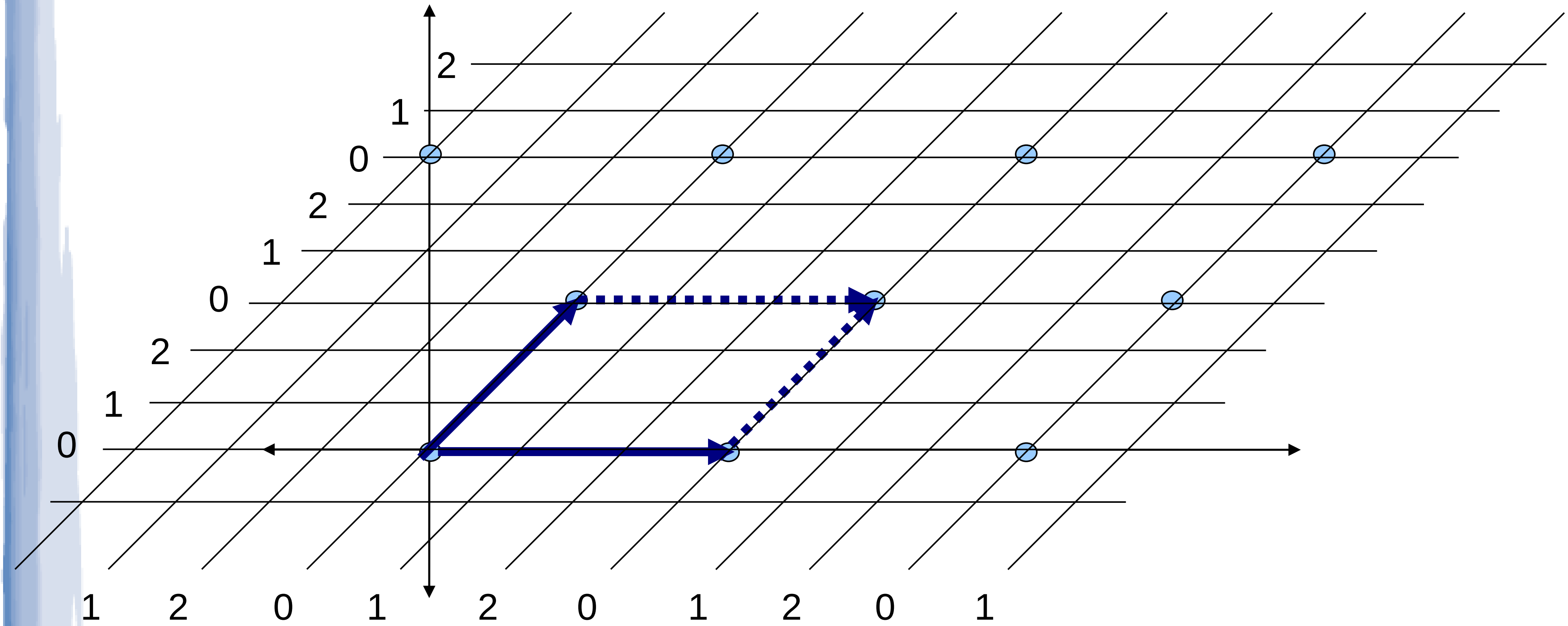
Worst-Case to Average-Case Reduction



Worst-Case to Average-Case Reduction



Worst-Case to Average-Case Reduction

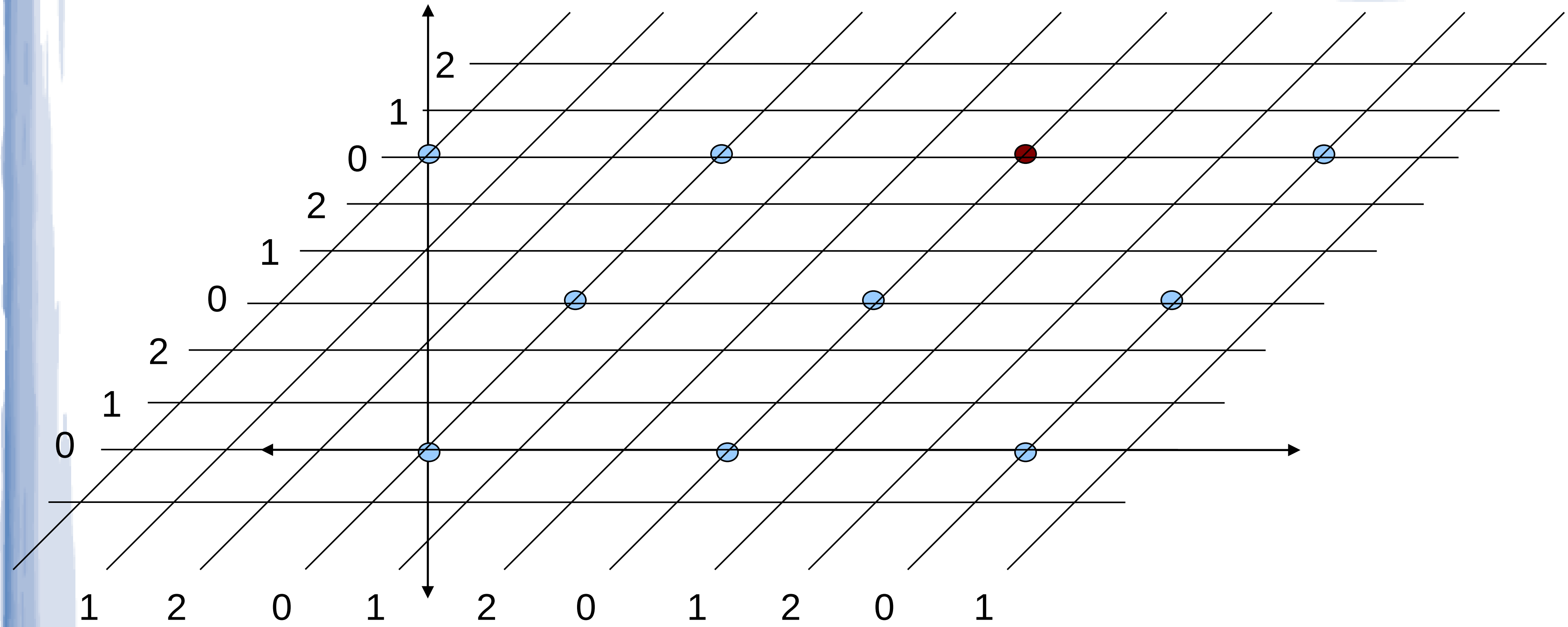


Important: All lattice points have label (0,0)

and

All points labeled (0,0) are lattice points

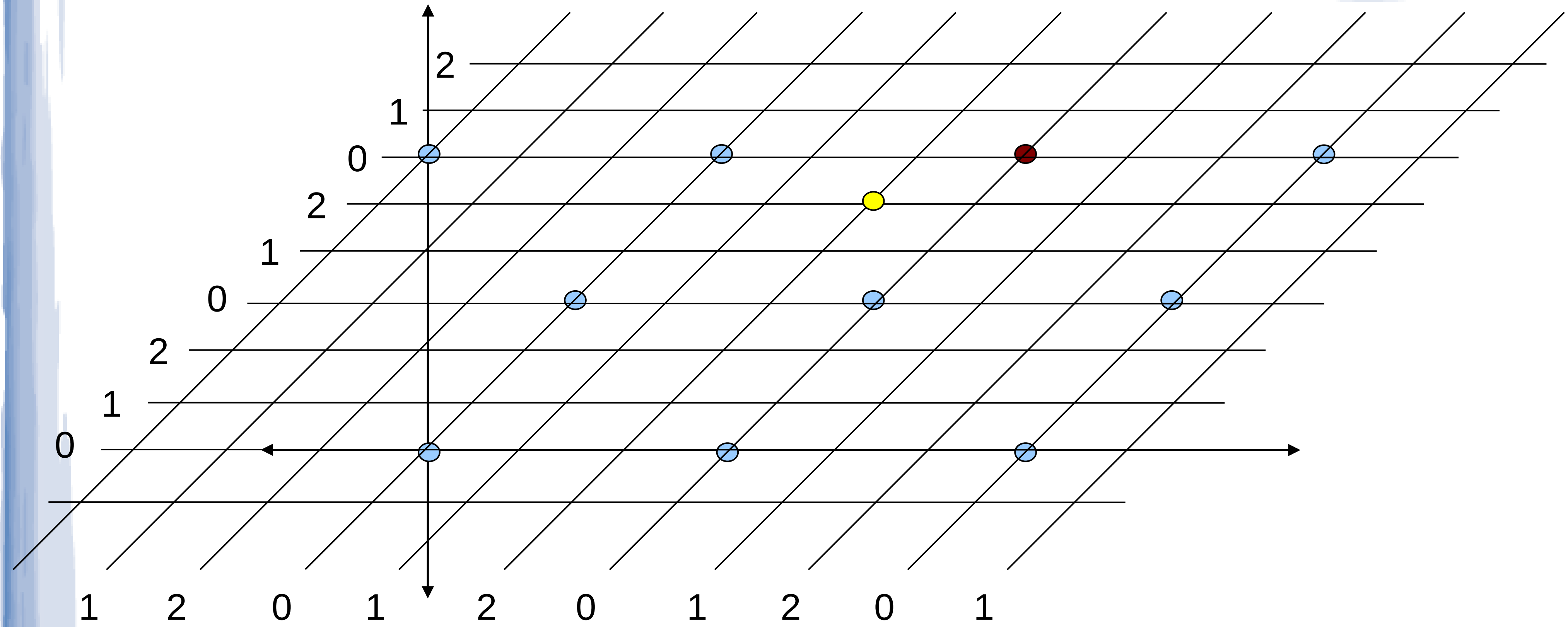
(0^n in n dimensional lattices)



<u>How to use the SIS oracle to find a short vector in any lattice:</u>

Repeat m times:

Pick a random lattice point

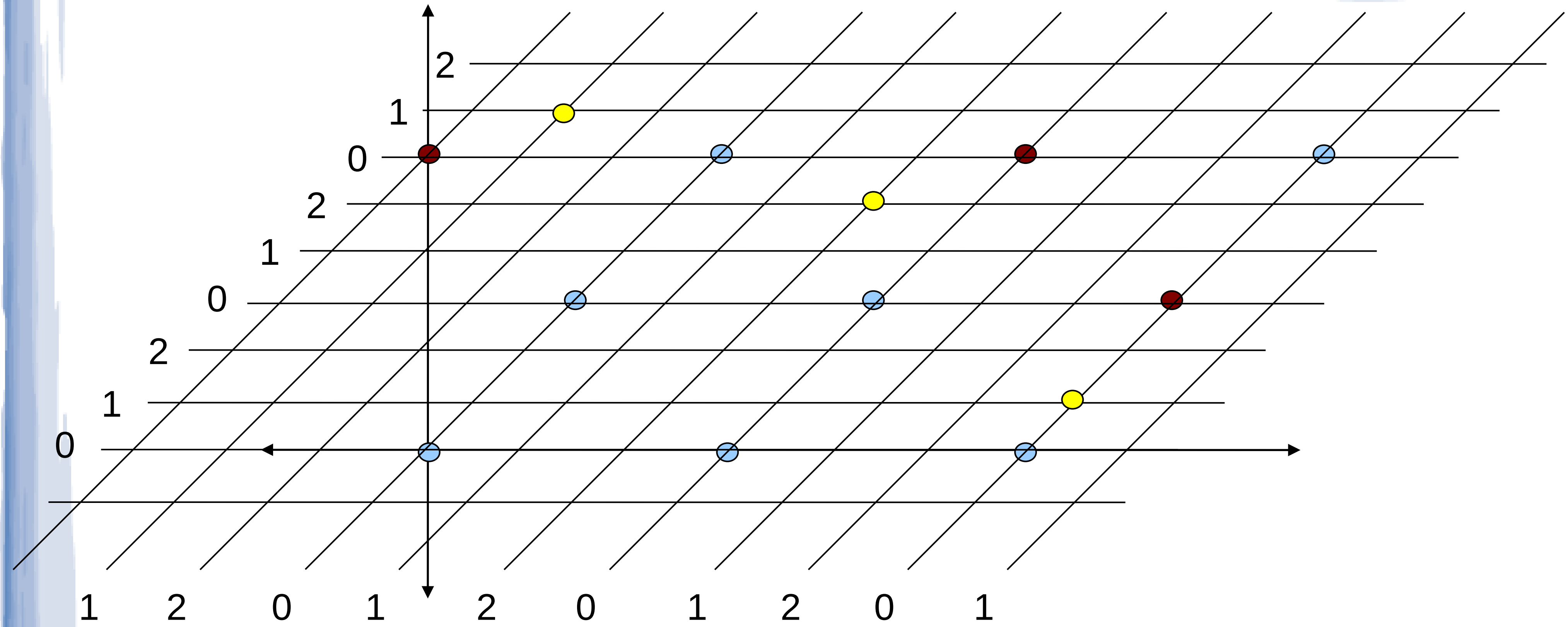


How to use the SIS oracle to find a short vector in any lattice:

Repeat m times:

Pick a random lattice point

Gaussian sample a point around the lattice point



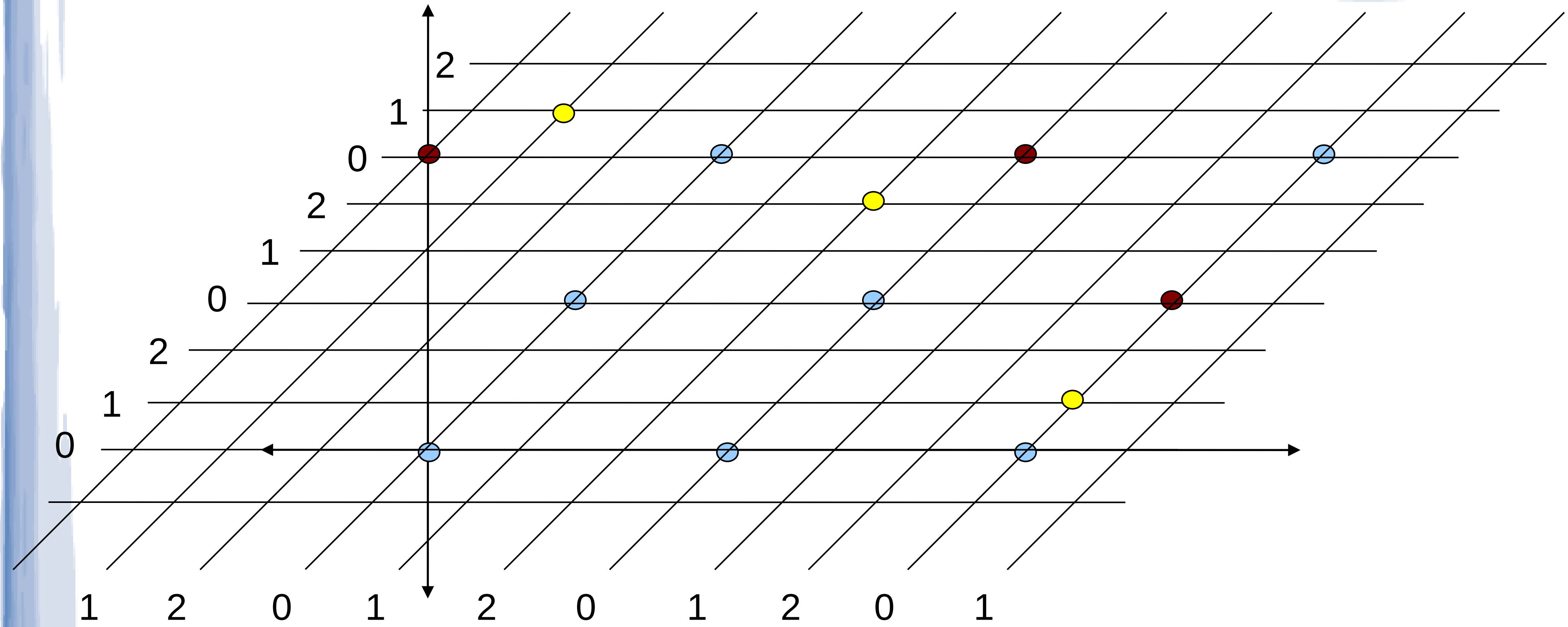
How to use the SIS oracle to find a short vector in any lattice:

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:

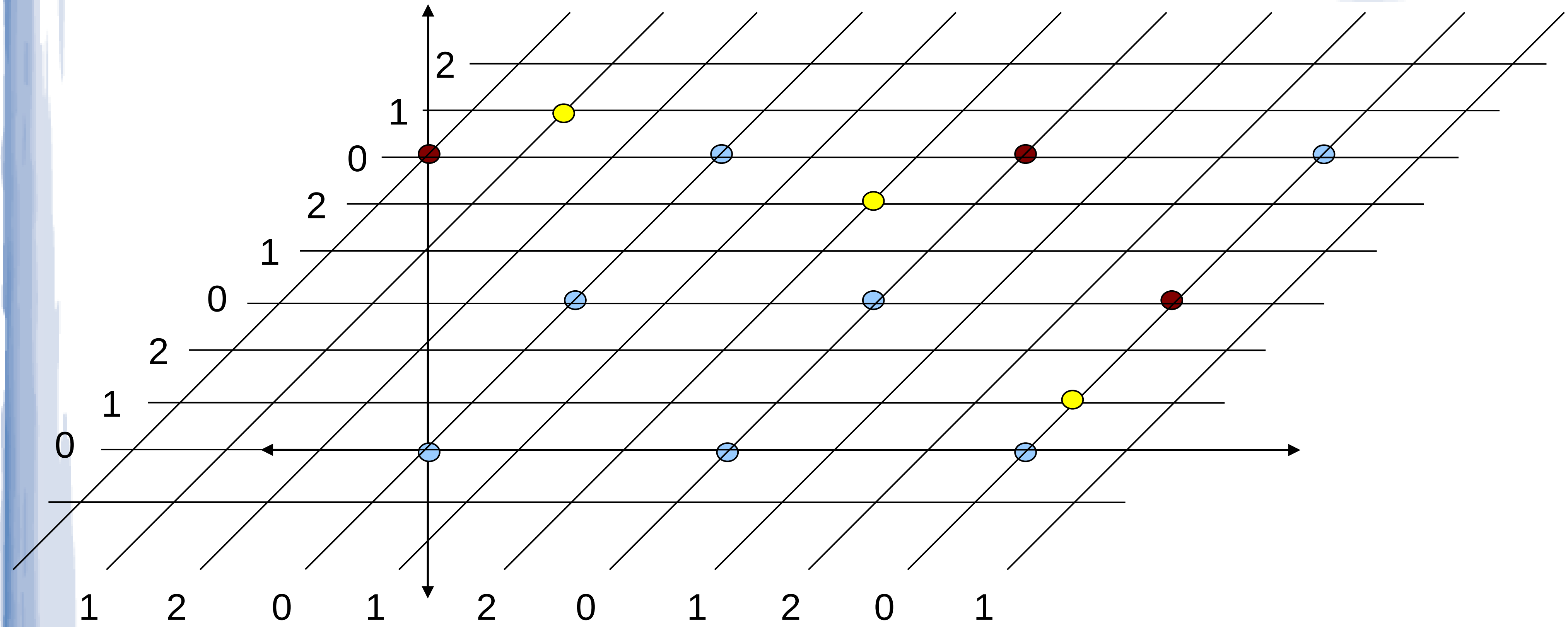
Repeat m times:

Pick a random lattice point

Gaussian sample a point around the lattice point

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

Oracle outputs $z_1,\ldots,z_m$ in {-1,0,1} such that $a_1z_1 + \ldots + a_mz_m = 0$



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

Oracle outputs $z_1,\ldots,z_m$ in {-1,0,1} such that $a_1z_1 + \ldots + a_mz_m = 0$

● $= v_i$

● $= s_i$

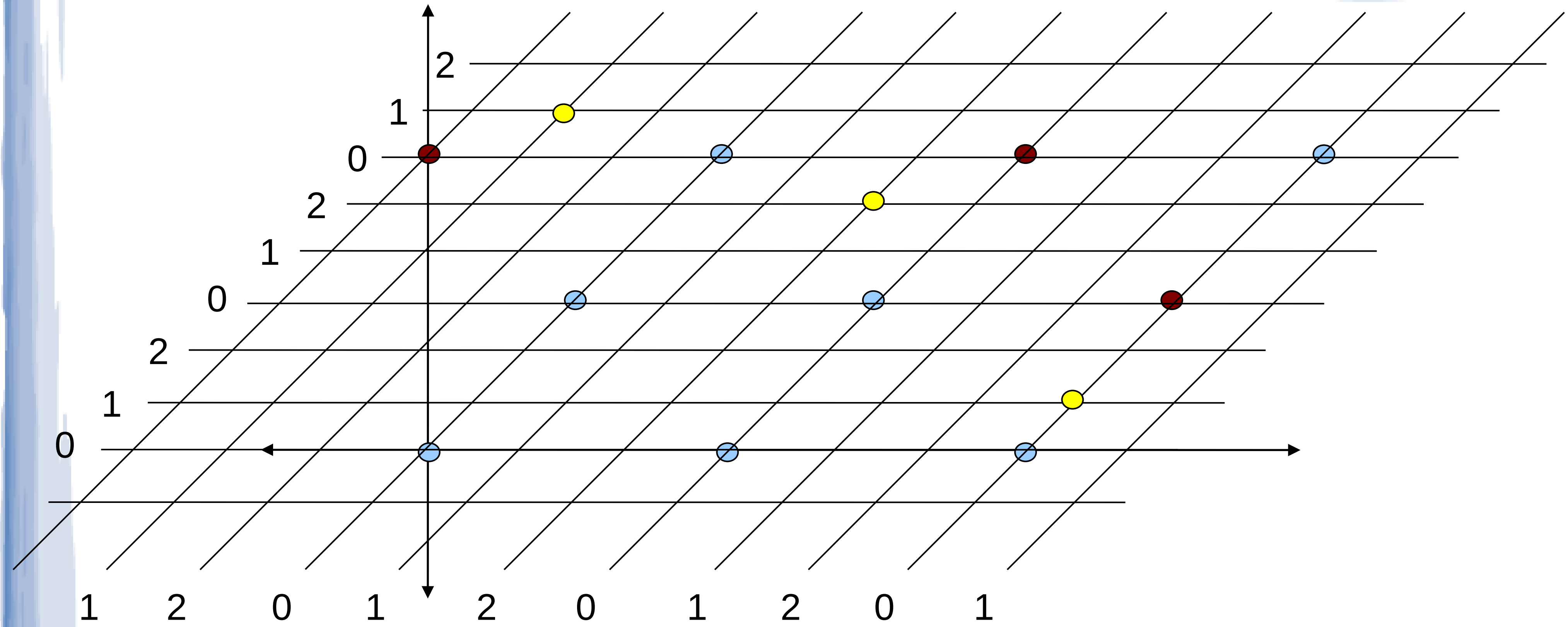
$v_i + r_i = s_i$

$s_1z_1+\ldots+s_mz_m$ is a lattice vector

$(v_1+r_1)z_1+\ldots+(v_m+r_m)z_m$ is a lattice vector

$(v_1z_1+\ldots+v_mz_m) + (r_1z_1+\ldots+r_mz_m)$ is a lattice vector

So $r_1z_1+\ldots+r_mz_m$ is a lattice vector



Give the m "Z_q^n samples" $a_1,\ldots,a_m$ to the SIS oracle

Oracle outputs $z_1,\ldots,z_m$ in $\{-1,0,1\}$ such that $a_1z_1 + \ldots + a_mz_m = 0$

● $= v_i$

● $= s_i$

$v_i + r_i = s_i$

So $r_1z_1+\ldots+r_mz_m$ is a lattice vector

r_i are short vectors, z_i are in $\{-1,0,1\}$

So $r_1z_1+\ldots+r_mz_m$ is a **short** lattice vector

Some Technicalities

- You can't sample a "uniformly random" lattice point
  - In the proofs, we work with $\mathbf{R}^n$ / L rather than $\mathbf{R}^n$
  - So you don't need to sample a random point lattice point
- What if $r_1z_1+\ldots+r_mz_m$ is 0?
  - Can show that with high probability it isn't
  - Given an s_i, there are multiple possible r_i
- Gaussian sampling doesn't give us points on the grid
  - You can round to a grid point
  - Must be careful to bound the "rounding distance"