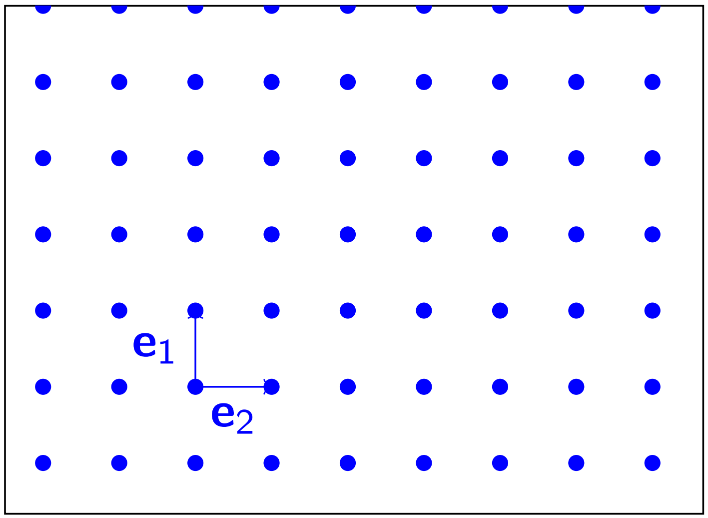
CS 6846
Quantum Algortithms and Cryptography

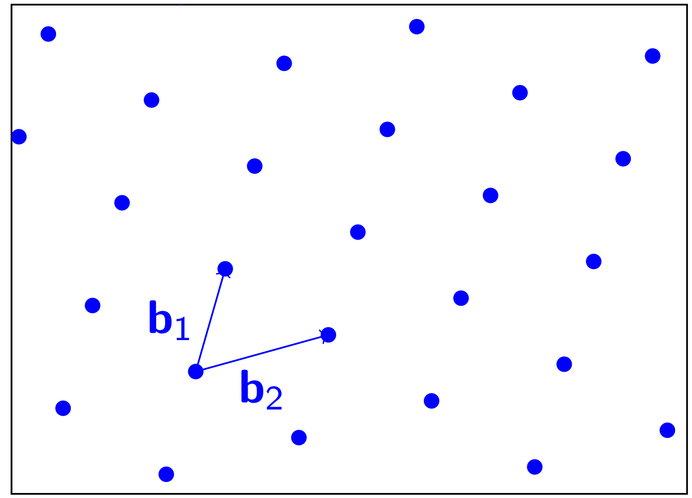
Shweta Agrawal
IIT Madras

What is a lattice?



The simplest lattice in n-dimensional space is the integer lattice

$$\Lambda = \mathbb{Z}^n$$



Other lattices are obtained by applying a linear transformation

$$\Lambda = \mathbf{B}\mathbb{Z}^n \qquad (\mathbf{B} \in \mathbb{R}^{d \times n})$$

A set of points with periodic arrangement

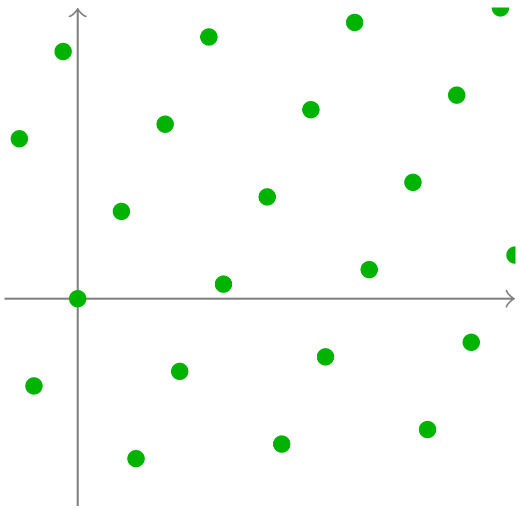
Lattices and Bases

A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{Bx} \colon \mathbf{x} \in \mathbb{Z}^n\}$$

The same lattice has many bases

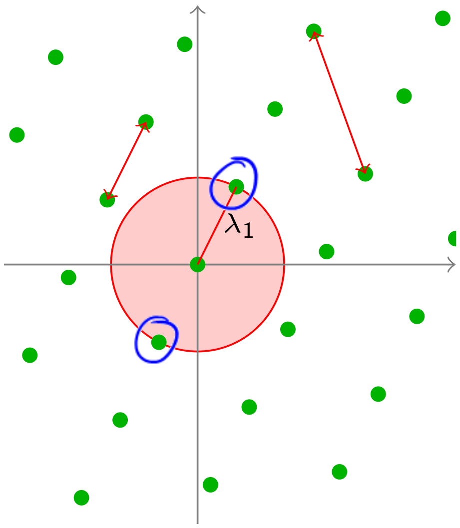
$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{c}_i \cdot \mathbb{Z}$$



Minimum Distance and Successive Minima

- Minimum distance

$$\lambda_1 = \min_{\mathbf{x},\mathbf{y}\in\mathcal{L},\mathbf{x}\neq\mathbf{y}} \|\mathbf{x}-\mathbf{y}\| = \min_{\mathbf{x}\in\mathcal{L},\mathbf{x}\neq\mathbf{0}} \|\mathbf{x}\|$$



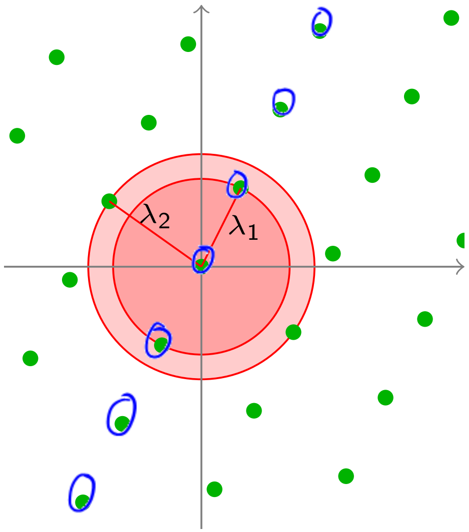
- Successive minima $(i = 1, \ldots, n)$

$$\lambda_i = \min\{r : \dim \operatorname{span}(\mathcal{B}(r)\cap\mathcal{L}) \geq i\}$$

Minimum Distance and Successive Minima

- Minimum distance

$$\lambda_1 = \min_{\mathbf{x},\mathbf{y}\in\mathcal{L},\mathbf{x}\neq\mathbf{y}} \|\mathbf{x}-\mathbf{y}\| = \min_{\mathbf{x}\in\mathcal{L},\mathbf{x}\neq\mathbf{0}} \|\mathbf{x}\|$$



- Successive minima ($i = 1, \ldots, n$)

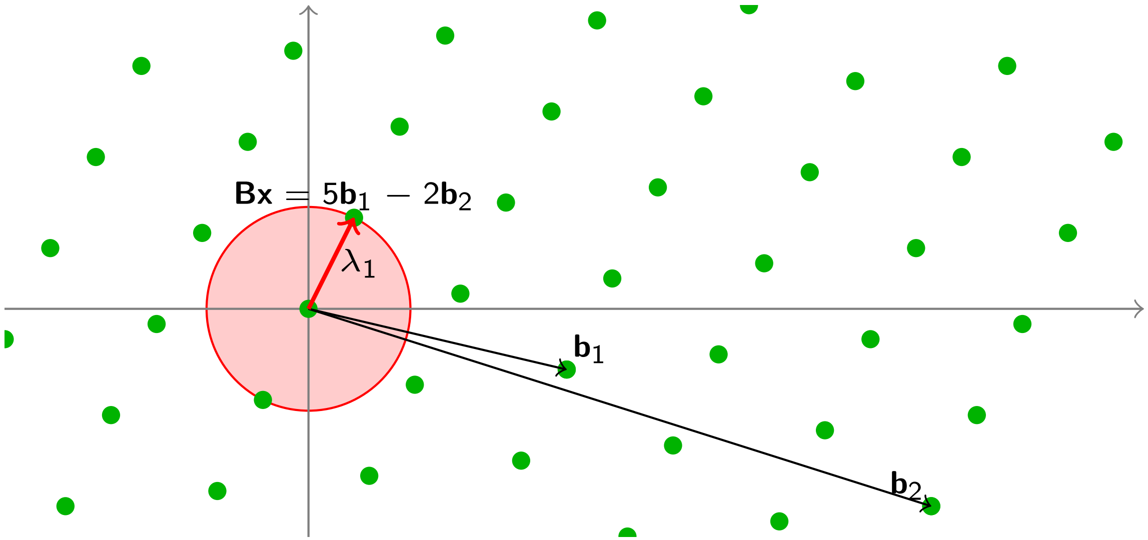
$$\lambda_i = \min\{r : \dim \operatorname{span}(\mathcal{B}(r) \cap \mathcal{L}) \geq i\}$$

- Examples
  - $\mathbb{Z}^n$: $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 1$
  - Always: $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$

Shortest Vector Problem

Definition (Shortest Vector Problem, SVP)

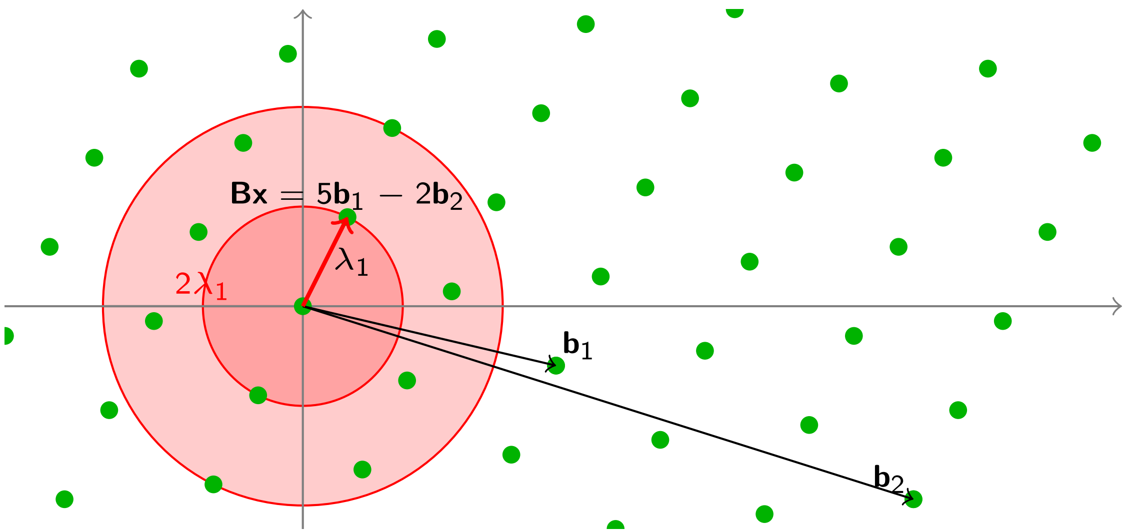
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



Approximate Shortest Vector Problem

Definition (Shortest Vector Problem, SVP$_\gamma$)

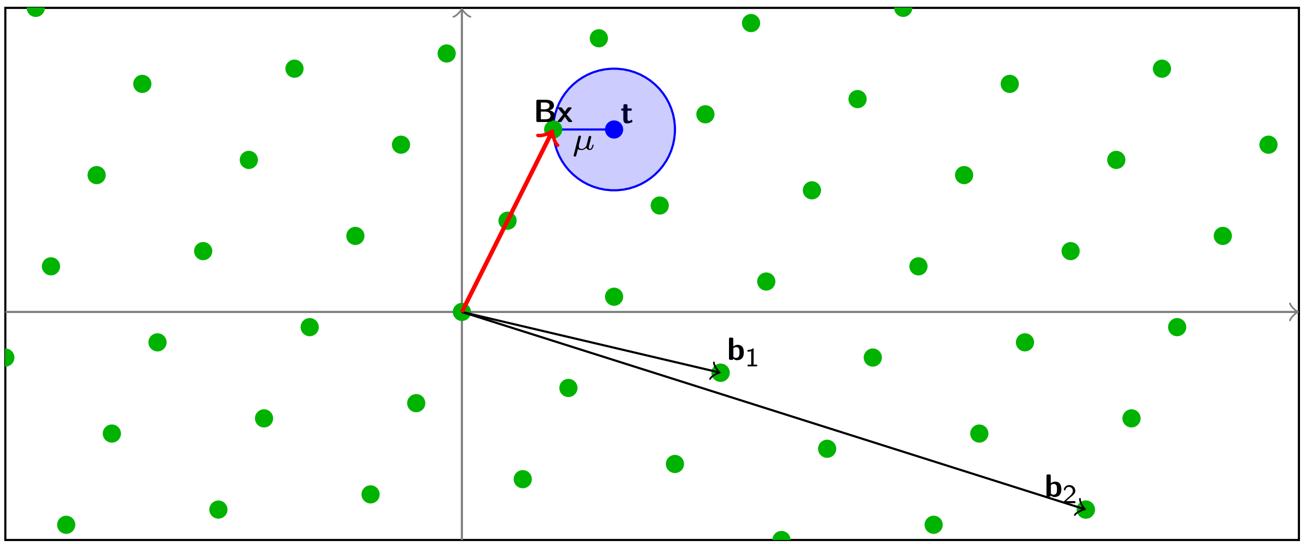
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \gamma\lambda_1$



Closest Vector Problem

Definition (Closest Vector Problem, CVP)

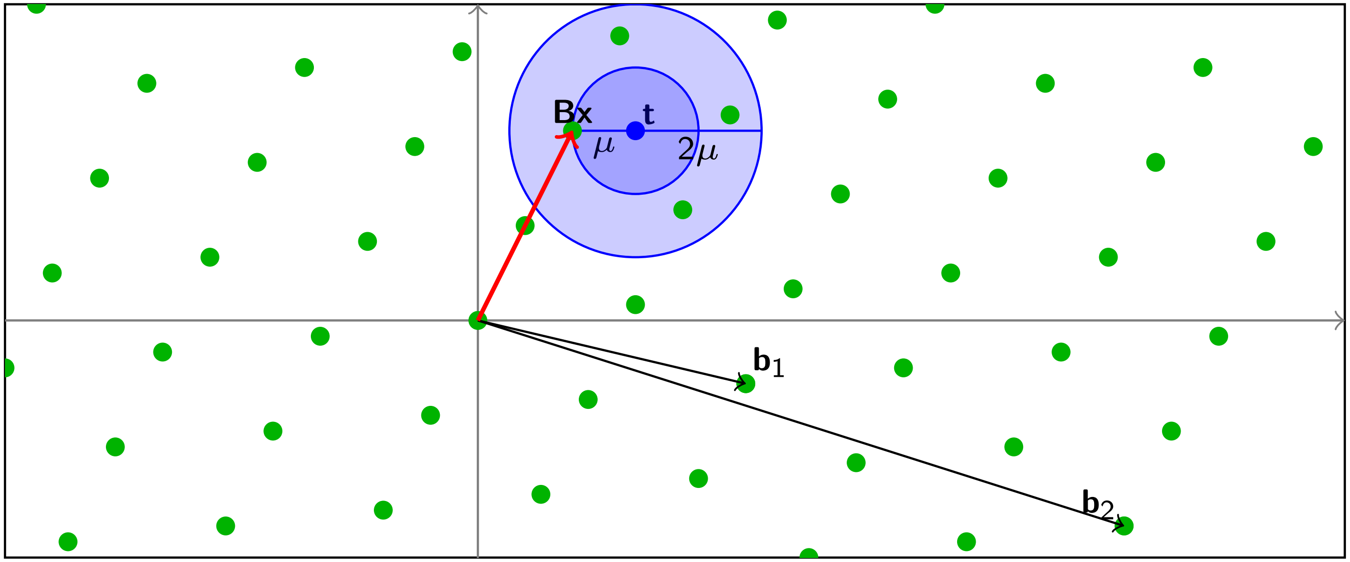
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \mu$ from the target



Approximate Closest Vector Problem

Definition (Closest Vector Problem, CVP_γ)

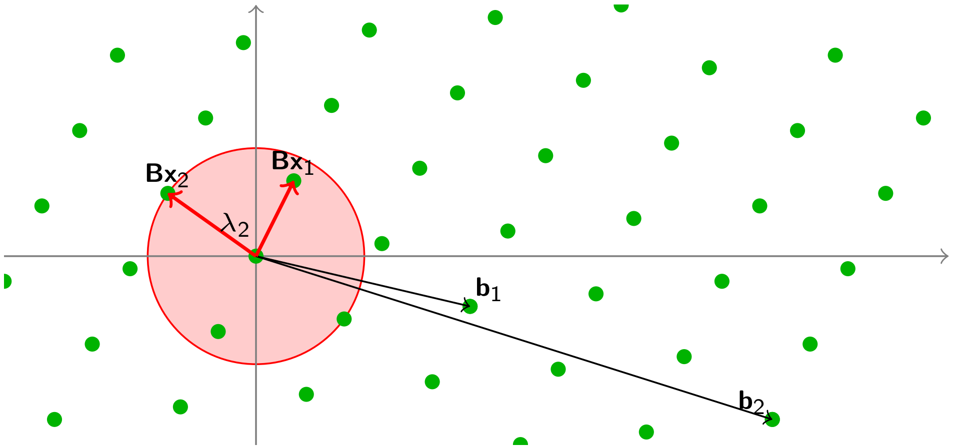
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma\mu$ from the target



Shortest Independent Vectors Problem

Definition (Shortest Independent Vectors Problem, SIVP)

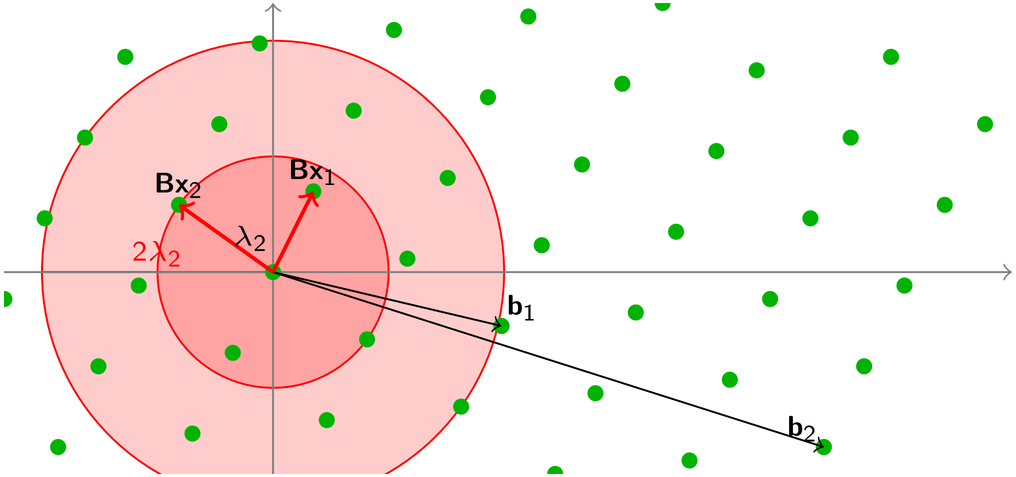
Given a lattice $\mathcal{L}(\mathbf{B})$, find n linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \lambda_n$



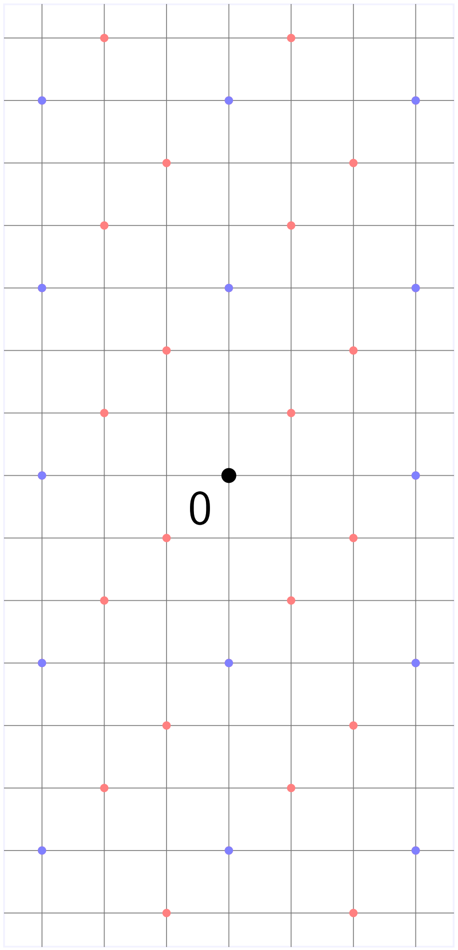
Approximate Shortest Independent Vectors Problem

Definition (Shortest Independent Vectors Problem, SIVP_γ)

Given a lattice $\mathcal{L}(\mathbf{B})$, find n linearly independent lattice vectors $\mathbf{B}\mathbf{x}_1, \ldots, \mathbf{B}\mathbf{x}_n$ of length (at most) $\max_i \|\mathbf{B}\mathbf{x}_i\| \leq \gamma\lambda_n$



Random Lattices in Cryptography



- Cryptography typically uses (random) lattices Λ such that
  - $\Lambda \subseteq \mathbb{Z}^d$ is an integer lattice
  - $q\mathbb{Z}^d \subseteq \Lambda$ is periodic modulo a small integer q.
- Cryptographic functions based on q-ary lattices involve only arithmetic modulo q.

Definition (q-ary lattice)

Λ is a q-ary lattice if $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

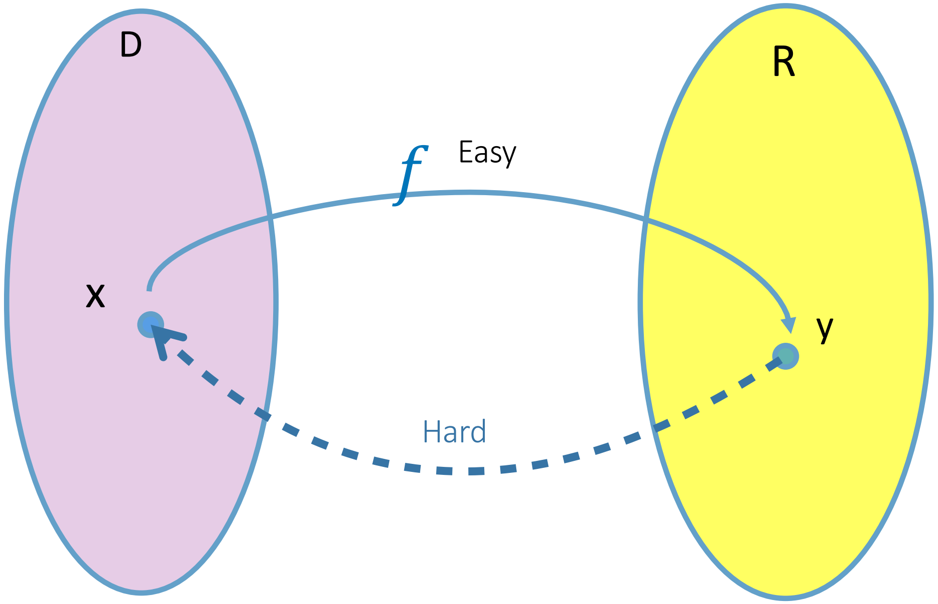
Examples (for any $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$)

- $\Lambda_q(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A}^T\mathbb{Z}_q^n\} \subseteq \mathbb{Z}^d$
- $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\} \subseteq \mathbb{Z}^d$ Perp

Building Cryptography

One Way Functions

$f: D \to R$, **One Way**

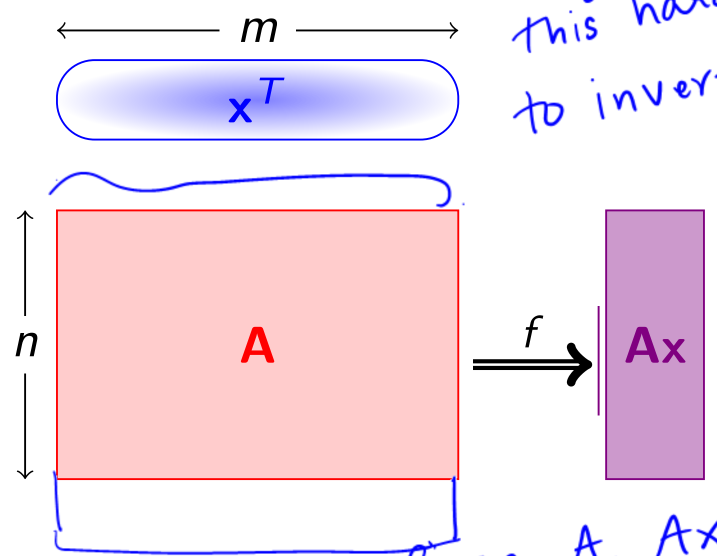


Most basic "primitive" in cryptography!

Ajtai's One Way Function

Why is this hard to invert?

- Parameters: $m, n, q \in \mathbb{Z}$
- Key: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$
- Input: $\mathbf{x} \in \underline{\{0,1\}^m}$ Binary.
- Output: $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$



$f_A : \underline{\{0,1\}^m} \to \mathbb{Z}_q^n$.

short vector

Given A, $Ax = y$

Find $\underline{x}$.

Theorem (A'96)

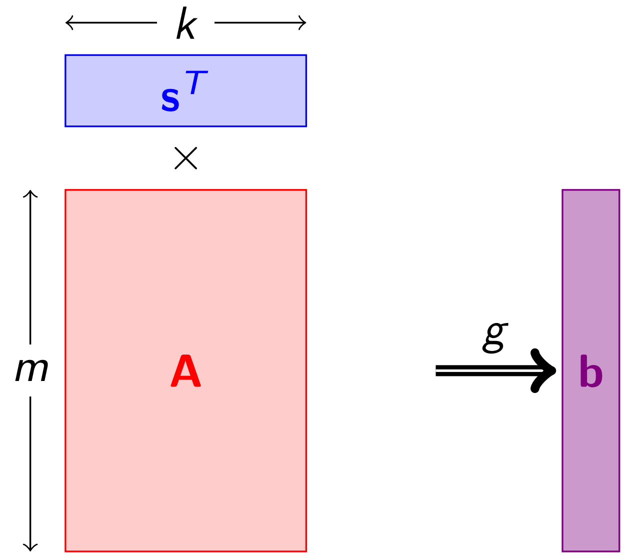
For $m > n \lg q$, if lattice problems (SIVP) are hard to approximate in the <u>worst-case</u>, then $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$ is a one-way function.

$m, n, q, A, y = Ax,$

Find x. (any x).

Regev's One Way Function

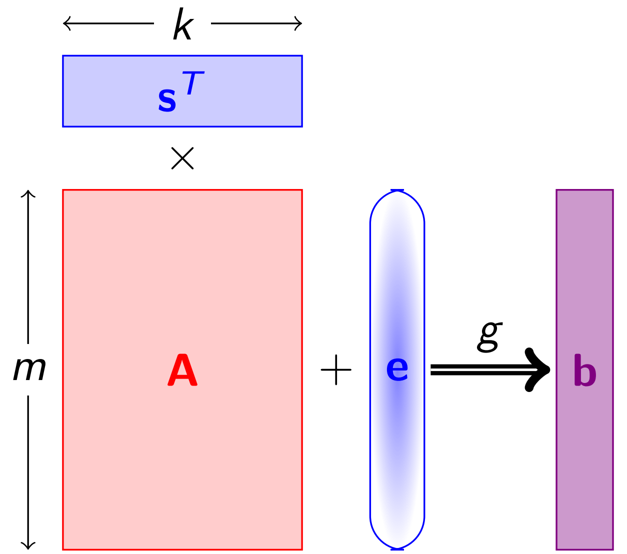
- $\mathbf{A} \in \mathbb{Z}_q^{m \times k}$, $\mathbf{s} \in \mathbb{Z}_q^k$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s}) = \mathbf{A}\mathbf{s} \mod q$



Regev's One Way Function

low norm (Binary)

- $\mathbf{A} \in \mathbb{Z}_q^{m \times k}$, $\mathbf{s} \in \mathbb{Z}_q^k$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s}; \mathbf{e}) = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
- Learning with Errors: Given $\mathbf{A}$ and $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$, recover $\mathbf{s}$.

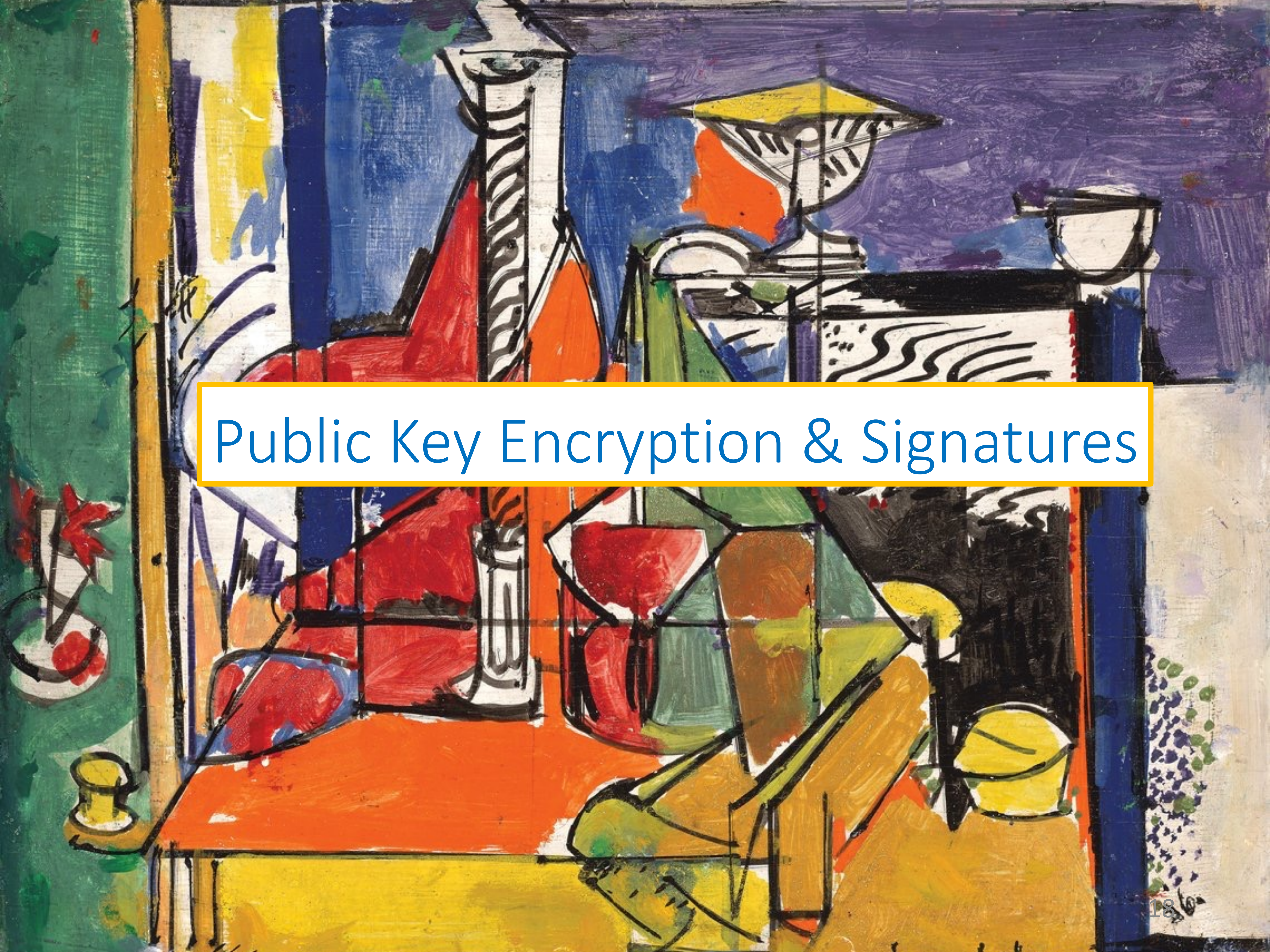


Theorem (R'05)

The function $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$ is hard to invert on the average, assuming SIVP is hard to approximate in the worst-case.

Given $\begin{cases} m, k, q. \\ A, \; y = As + e, \end{cases}$

Want: $\underline{\underline{s}}$.



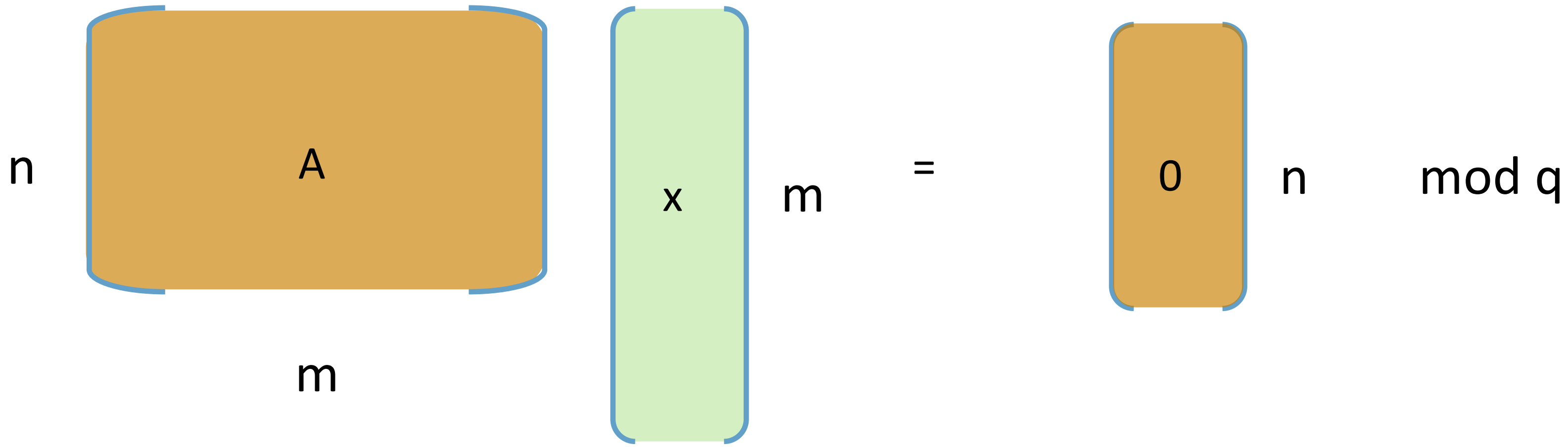
Public Key Encryption & Signatures

Short Integer Solution Problem

Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}, q = \text{poly}(n), m = \Omega(n \log q)$

Given matrix **A**, find "short" (low norm) vector **x** such that

$$\mathbf{Ax} = \underline{0} \ \ mod \ \ q \in \mathbb{Z}_q^n \qquad \|x\| \leq \beta$$



Learning With Errors Problem

Distinguish "noisy inner products" from uniform

Fix uniform $s \in Z_q^{\,n}$

some low norm distribution

a_1 , $b_1 = \langle a_1, s\rangle + e_1$

a_2 , $b_2 = \langle a_2, s\rangle + e_2$

$\vdots$

a_m , $b_m = \langle a_m, s\rangle + e_m$

vs

a'_1 , b'_1

a'_2 , b'_2

$\vdots$

a'_m , b'_m

a_i uniform $\in Z_q^{\,n}$, $e_i \sim \phi \in Z_q$

a_i uniform $\in Z_q^{\,n}$, b_i uniform $\in Z_q$

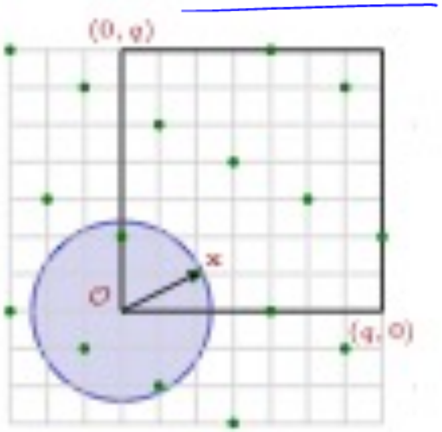
Recap:Lattice Based One Way Functions

$Public\ Key\ \mathbf{A} \in \mathbb{Z}_q^{n\times m}, q = \text{poly}(n), m = \Omega(n\log q)$

Ajtai's
Based on SIS

$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{Ax}\ mod\ q \in \mathbb{Z}_q^n$

- Short x, surjective
- CRHF if SIS is hard



Regev's
Based on LWE

$g_{\mathbf{A}}(\mathbf{s}, \mathbf{e}) = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t mod q \in \mathbb{Z}_q^m$

- Very short e, injective
- OWF if LWE is hard [Reg05…]

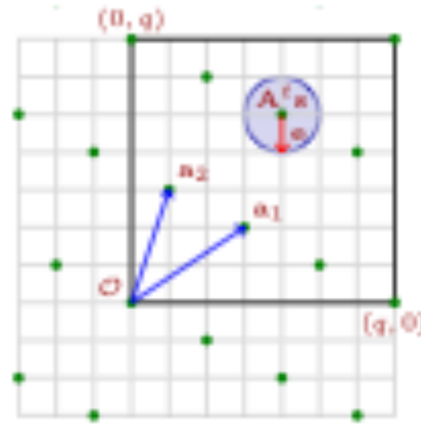


Image Credit: MP12 slides

Public Key Encryption [Regev05]

- Recall $A(e) = u \bmod q$ hard to invert
- Secret: e, Public : A, u

$$\boxed{A}\ \boxed{e} \equiv \boxed{u} \bmod q$$

- Encrypt (A, u) :
  - Pick random vector s
  - $c_0 = A^T s + \text{noise}$
  - $c_1 = u^T s + \text{noise} + \text{msg}$
- Decrypt (e) :
  - $e^T c_0 - c_1 = \text{msg} + \text{noise}$

Small only
if e is small

Public Key Encryption [Regev05]

- Recall $A(e) = u \bmod q$ hard to invert
- Secret: e, Public : A, u

$$A \, e \equiv u \mod q$$

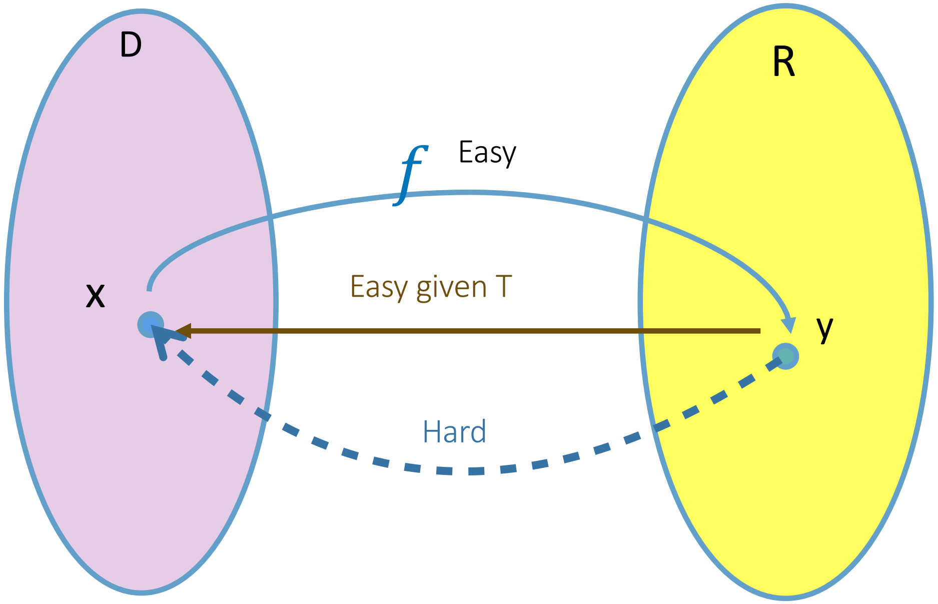
- By SIS problem, hard to find short e
- By LWE problem, ciphertext appears random
  - $c_0 = A^T s$ + noise, looks like random
  - $c_1 = u^T s$ + noise + msg , looks like random + msg
  - Hence hides message “msg”

For Signatures, need
Lattice Trapdoors

Trapdoor Functions

Generate (f, T)

$f: D \rightarrow R,$ One Way



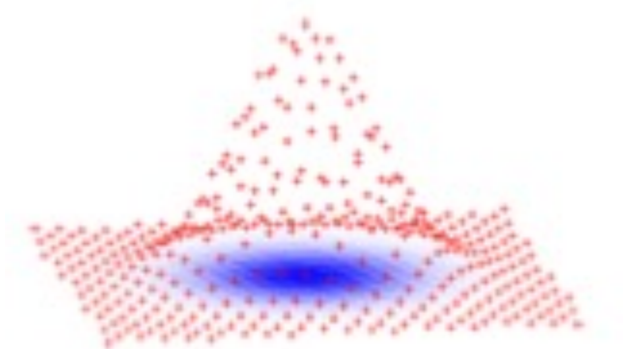
We will construct trapdoor functions from two lattice problems

Inverting functions for Crypto

- Given $\mathbf{u} = f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}\ mod q$
- Sample

$$\mathbf{x}' \leftarrow= f_{\mathbf{A}}^{-1}(\mathbf{u})$$

with prob $\propto \exp(-\| \mathbf{x}' \|^2/\sigma^2)$



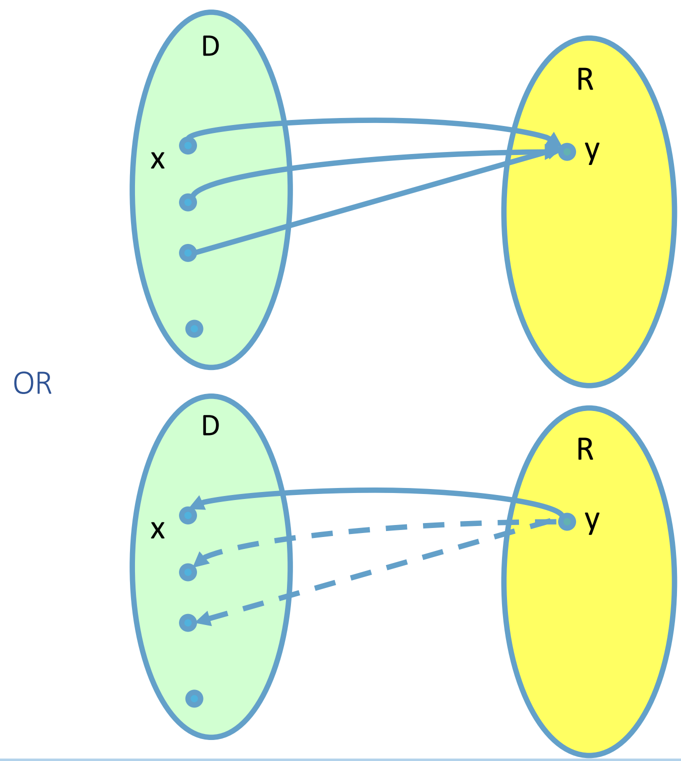
- (
- F

$nodq$

Latter distribution needs lattice trapdoors!

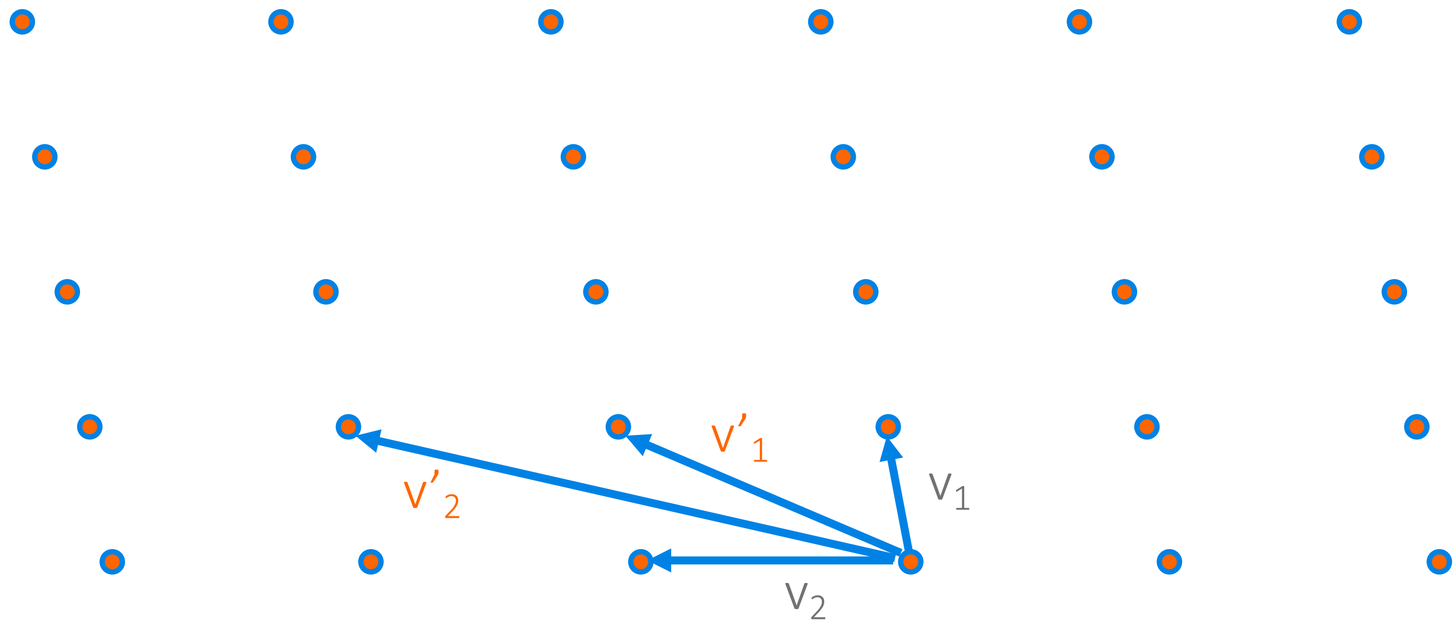
Preimage Sampleable Trapdoor Functions!

Generate (x, y) in two equivalent ways



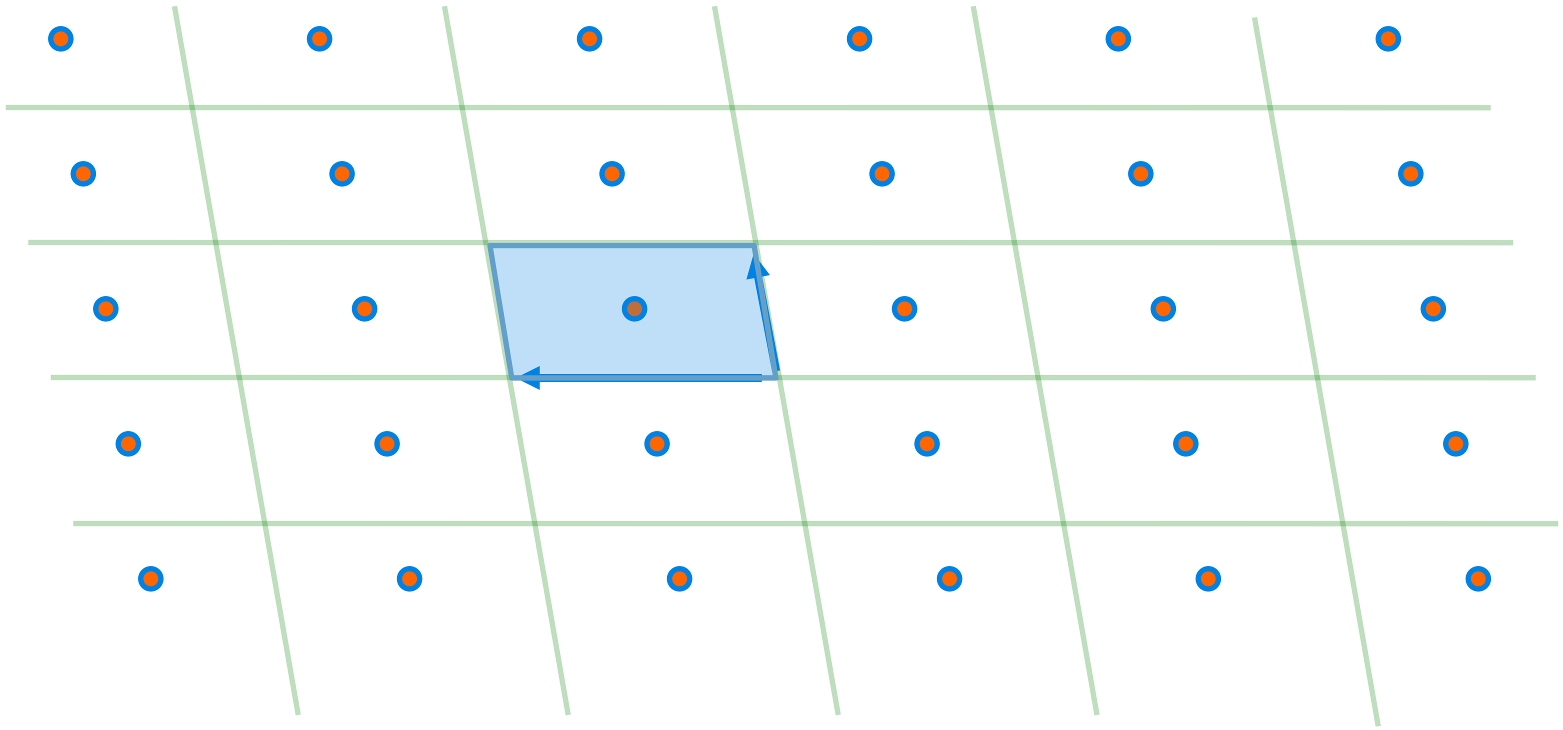
Same Distribution (Discrete Gaussian, Uniform) !

Lattice Trapdoors: Geometric View

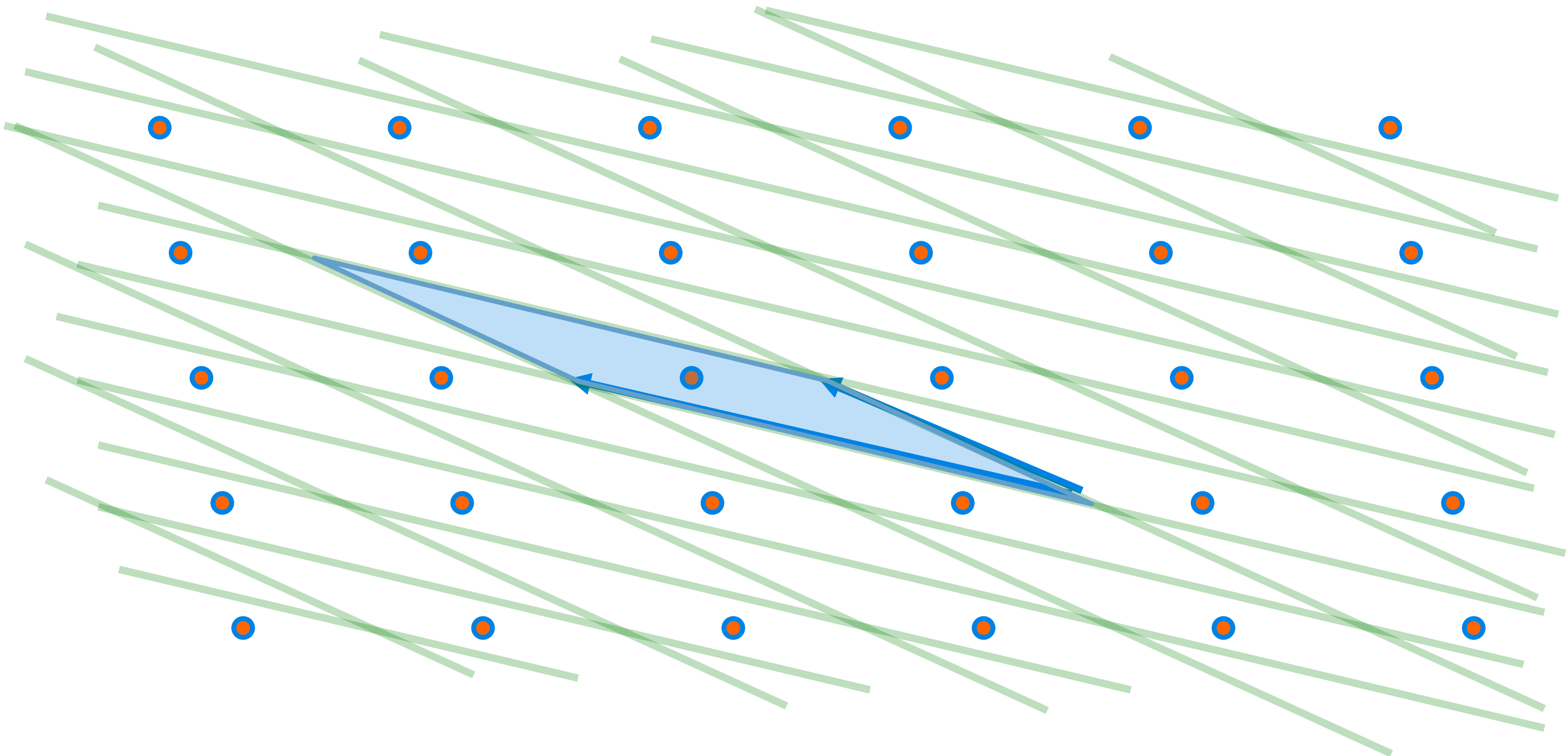


Multiple Bases

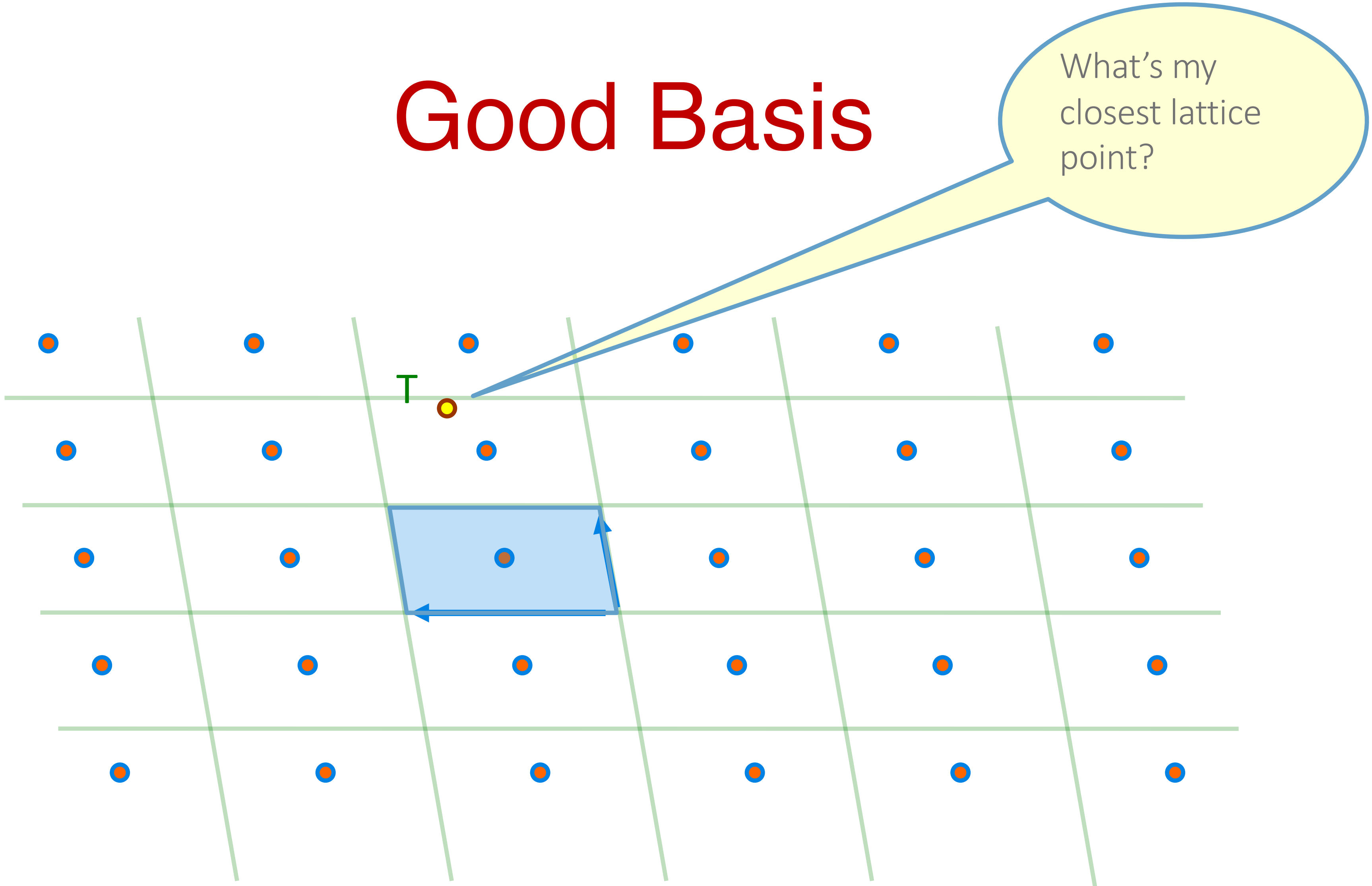
Parallelopipeds



Parallelopipeds

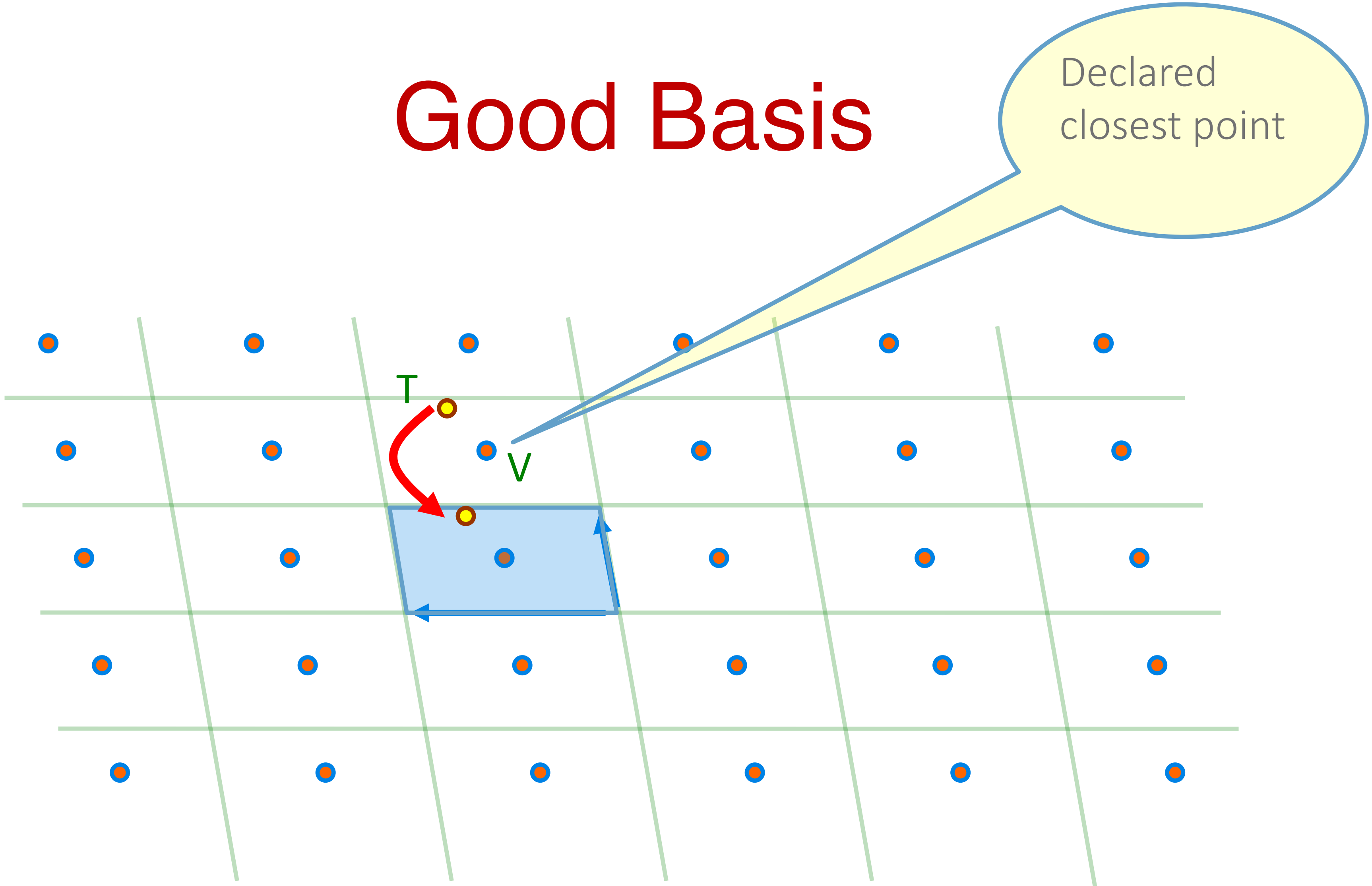


Good Basis



"Quite short" and "nearly orthogonal"

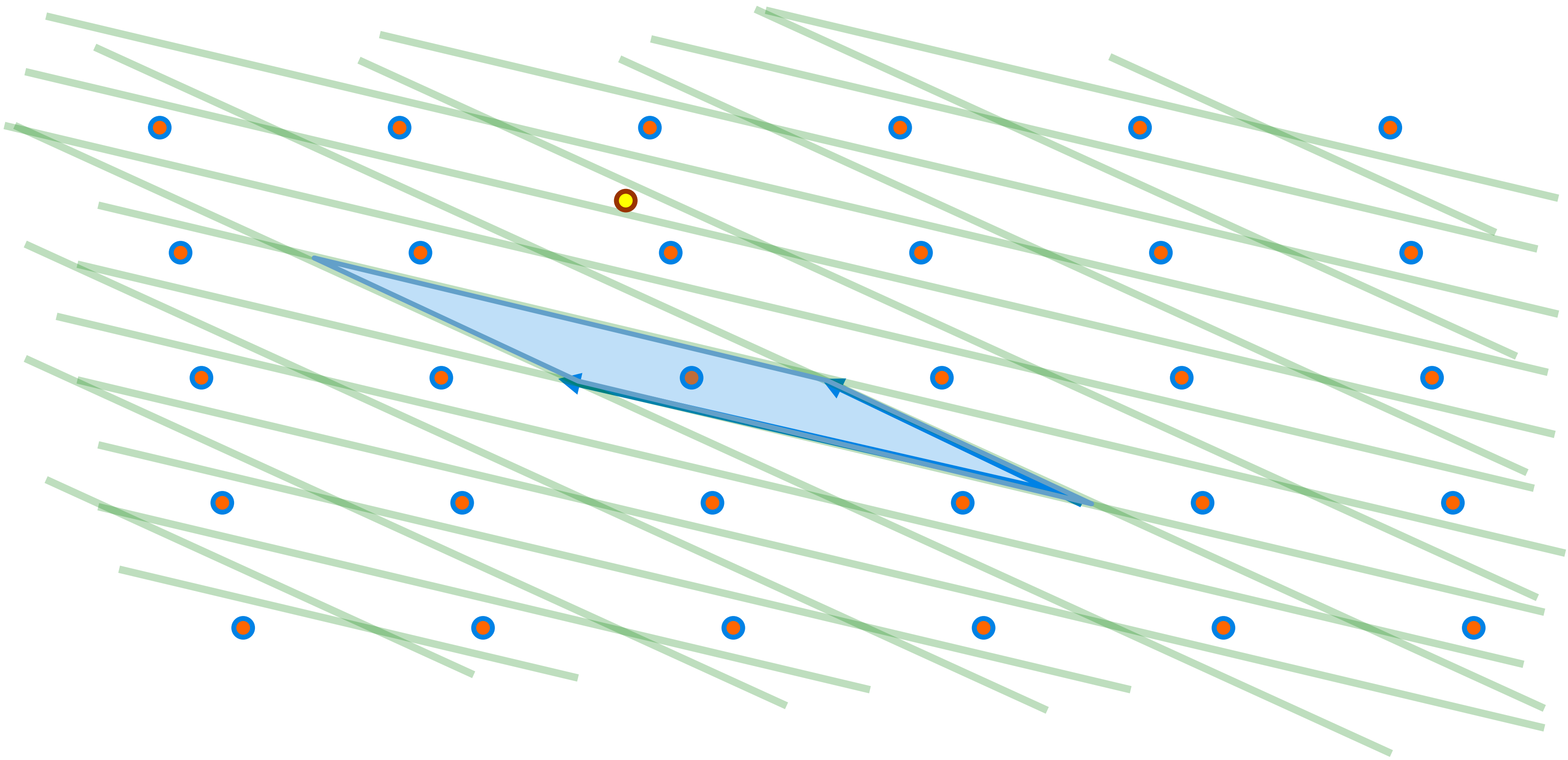
Good Basis



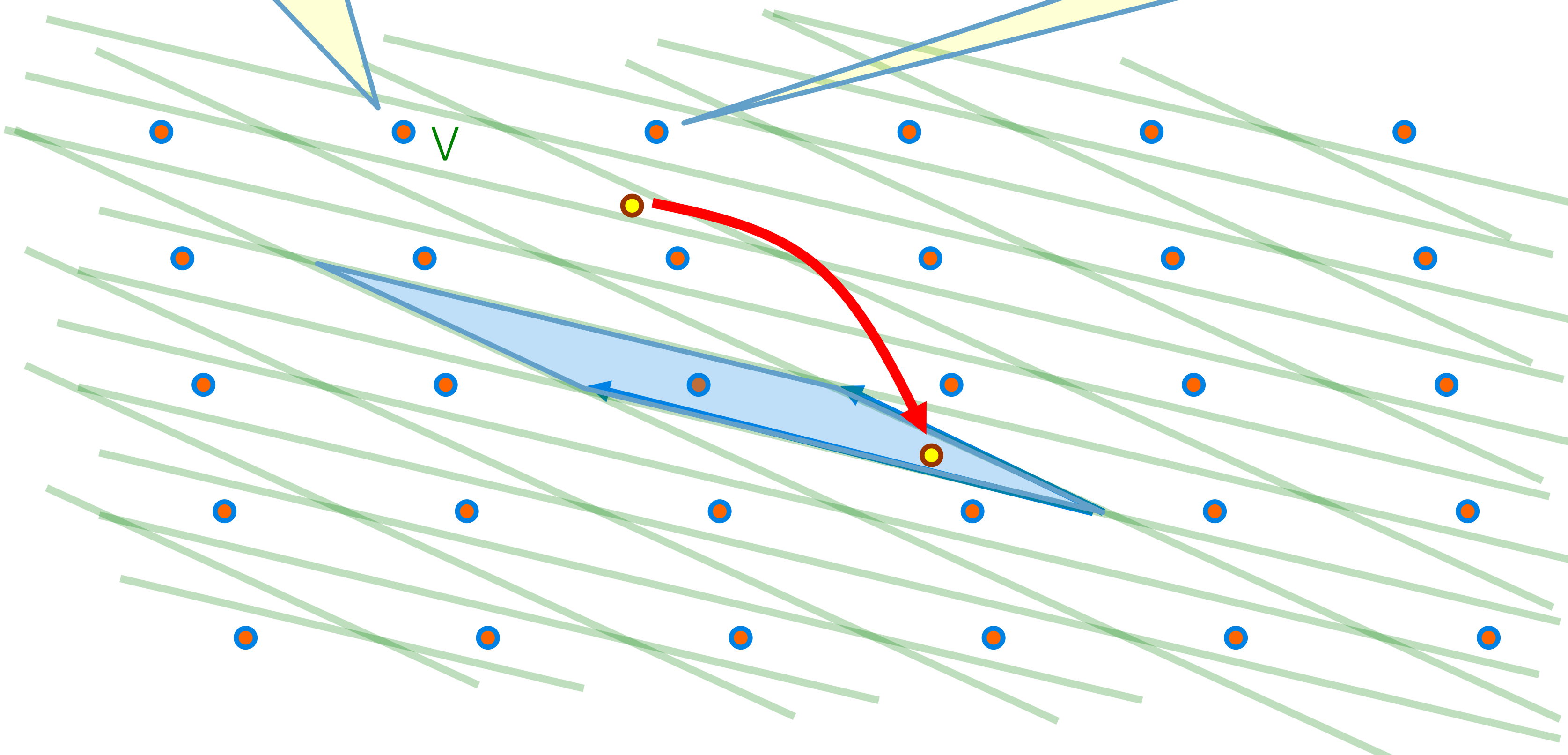
Output center of parallelopipid containing T

Pretty Accurate...

Bad Basis



Bad Basis



Output center of parallelopipid containing T

Not So Accurate…

Basis quality and Hardness

- SVP, CVP, SIS (...) hard given arbitrary (bad) basis
- Some hard lattice problems are easy given a good basis
- Will exploit this asymmetry

Use Short Basis as Cryptographic Trapdoor!

Lattice Trapdoors

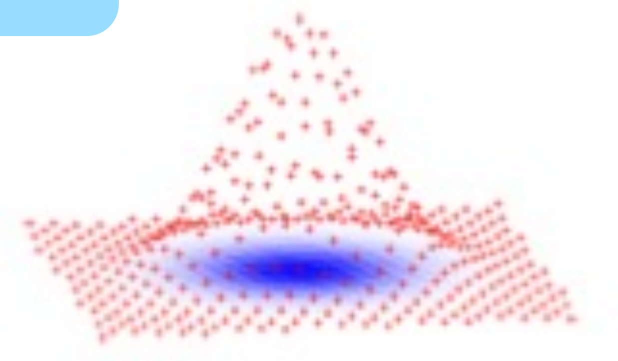
Inverting Our Function

Recall $\mathbf{u} = f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\,\mathbf{x}\, mod q$

Want

$$\mathbf{x}' \leftarrow= f_{\mathbf{A}}^{-1}(\mathbf{u})$$

with prob $\propto \exp(-\| \mathbf{x}' \|^2/\sigma^2)$

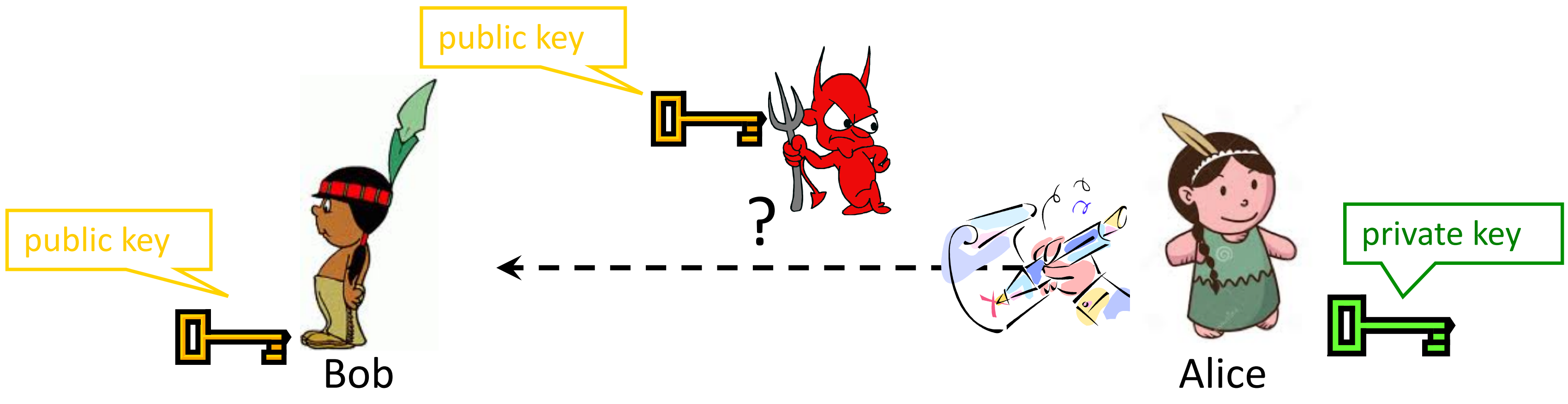


The Lattice

$$\mathbf{\Lambda} = \{\mathbf{x}: \mathbf{A}\mathbf{x} = 0 \; mod \; q\} \subseteq \mathbb{Z}_q^m$$

Short basis for $\mathbf{\Lambda}$ lets us sample from $f_{\mathbf{A}}^{-1}(\mathbf{u})$ with correct distribution!

Digital Signatures



Everybody knows Alice's public key
Only Alice knows the corresponding private key

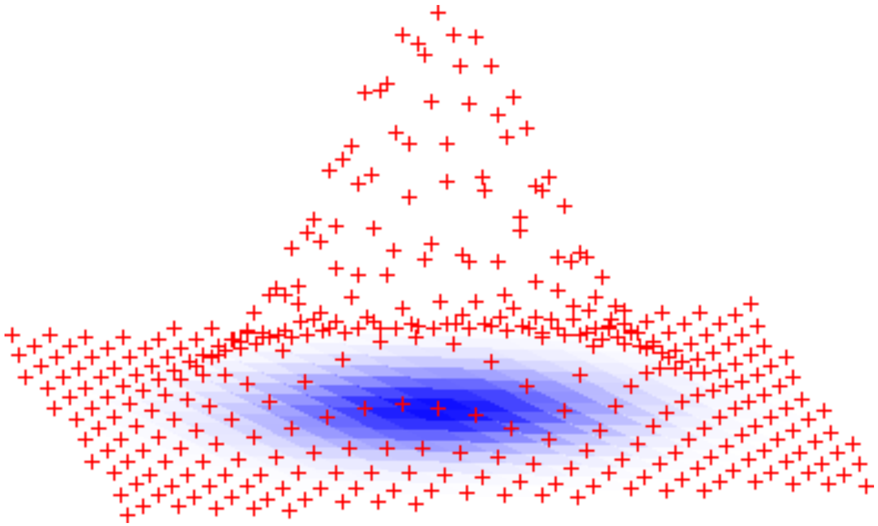
<u>Goal</u>: Alice sends a "digitally signed" message

1. To compute a signature, must know the private key
2. To verify a signature, only the public key is needed

Digital Signatures from Lattices

- Generate uniform $vk = \mathbf{A}$ with secret 'trapdoor' $sk = \mathbf{T}$.
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{z} = H(\mu) \in \mathbb{Z}_q^n$.

  Draw $\mathbf{z}$ from a distribution that reveals nothing about secret key:



- Verify$(\mathbf{A}, \mu, \mathbf{z})$: check that $\mathbf{A}\mathbf{z} = H(\mu)$ and $\mathbf{z}$ is sufficiently short.
- Security: forging a signature for a new message μ^* requires finding short $\mathbf{z}^*$ s.t. $\mathbf{A}\mathbf{z}^* = H(\mu^*)$. This is SIS: hard!

Summary

- Basics of Lattices
- Hard Problems on Lattices
- Public Key Encryption
- Lattice Trapdoors
- Digital Signatures

Thank You

Images Credit: Hans Hoffman

Slides Credit: Daniele Micciancio, Chris Peikert