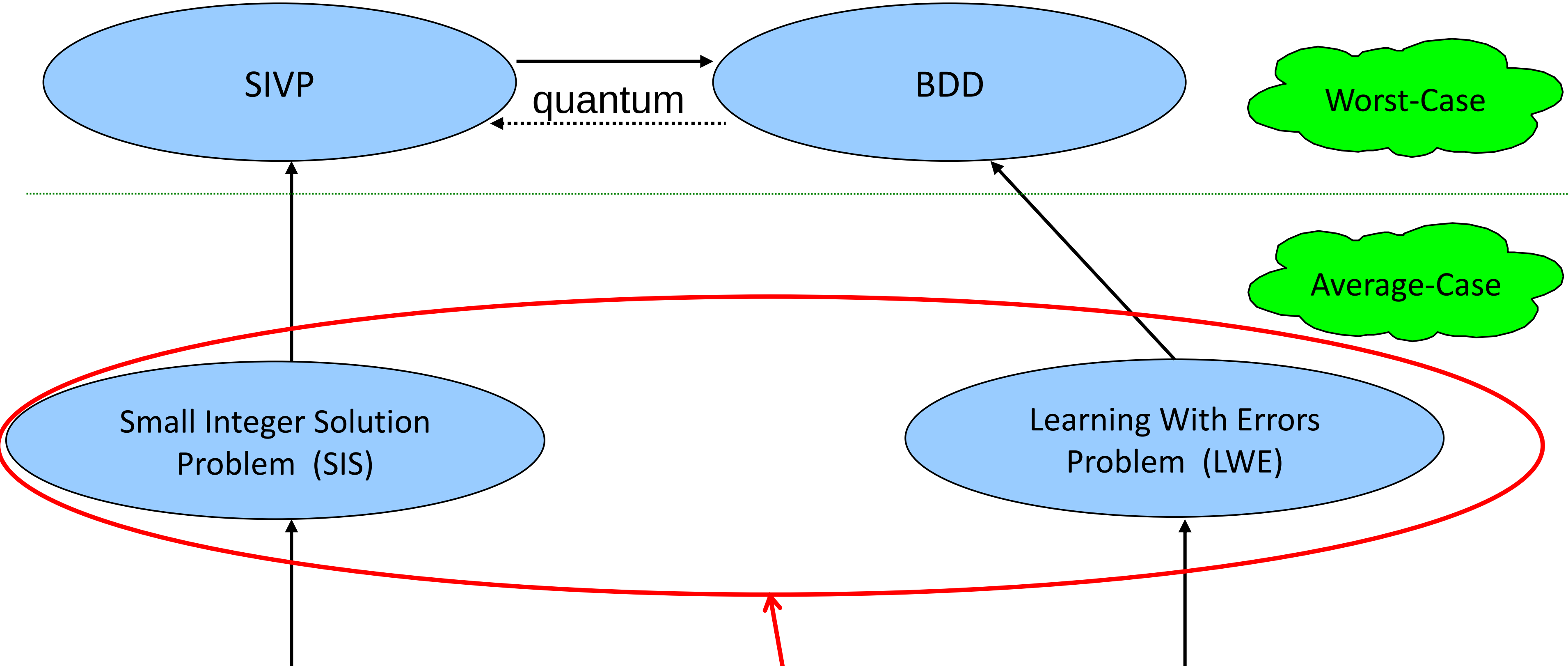
Basic Cryptanalysis

Vadim Lyubashevsky

INRIA / ENS, Paris

Outline

- LLL sketch
- Application to Subset Sum
- Application to SIS
- Application to LWE
- Lattice Reduction in Practice



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

(Minicrypt)

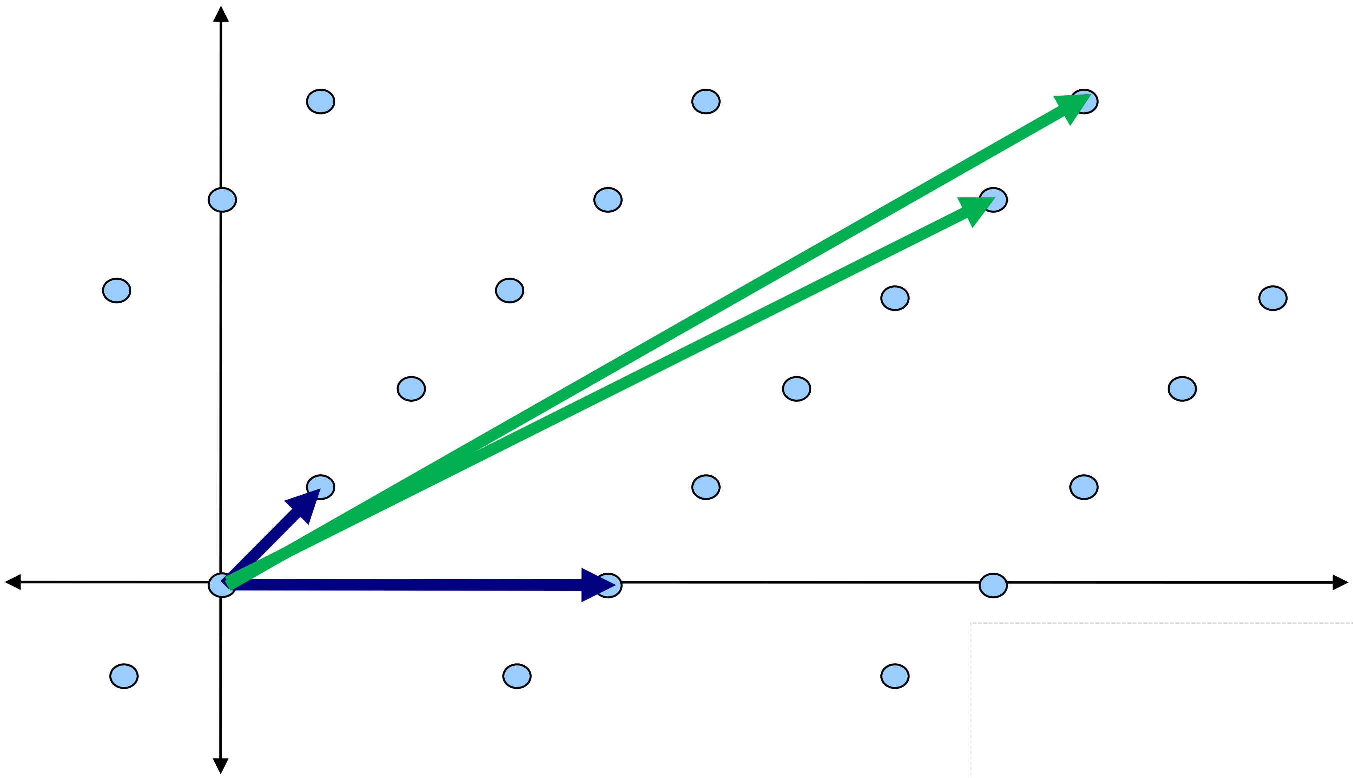
Public Key Encryption …
(Cryptomania)

How hard are these problems??

LLL

[Lenstra, Lenstra, Lovasz ‘82]

Lattice Bases



The Goal of Lattice Reduction

Obtain a basis **B** in which the Gram-Schmidt vectors are not decreasing too quickly

This roughly means that the basis vectors are somewhat orthogonal to each other

LLL Reduced Basis $\mathbf{B}$

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

$\mu_{i,j} = (\mathbf{b}_i \cdot \tilde{\mathbf{b}}_j)/||\tilde{\mathbf{b}}_j||^2$

<u>An LLL-reduced basis has:</u>

$$\left.\begin{array}{l} \text{1. All } |\mu_{i,j}| \leq 0.5 \\ \\ \text{2. } 0.75||\tilde{\mathbf{b}}_i||^2 \leq ||\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}||^2 \end{array}\right\} ||\tilde{\mathbf{b}}_{i+1}||^2 \geq 0.5||\tilde{\mathbf{b}}_i||^2$$

Short Vector in an LLL-reduced Basis

Thm: The vector $\mathbf{b_1}$ in an LLL-reduced basis has length at most $2^{(n-1)/2} \cdot \lambda_1(L(\mathbf{B}))$

Proof:

$||\tilde{\mathbf{b}}_{\mathbf{n}}||^2 \geq 0.5||\tilde{\mathbf{b}}_{\mathbf{n-1}}||^2 \geq \ldots \geq 0.5^{n-1}||\tilde{\mathbf{b}}_{\mathbf{1}}||^2 = 0.5^{n-1}||\mathbf{b_1}||^2$

$||\mathbf{b_1}|| \leq 2^{(n-1)/2}||\tilde{\mathbf{b}}_{\mathbf{i}}||$ for all i

Since, $\min_i ||\tilde{\mathbf{b}}_{\mathbf{i}}|| \leq \lambda_1(L(\mathbf{B}))$, we have

$$||\mathbf{b_1}|| \leq 2^{(n-1)/2} \cdot \lambda_1(L(\mathbf{B}))$$

LLL Algorithm

$$\begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \mathbf{b_1} & \mathbf{b_2} & \mathbf{b_3} & \cdots & \mathbf{b_n} \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix} = \begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \tilde{\mathbf{b}}_3 & \cdots & \tilde{\mathbf{b}}_n \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix} \begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & \cdots & \mu_{n,2} \\ \cdots & 0 & 1 & \cdots & \mu_{n,3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

An LLL-reduced basis has:

1. All $|\mu_{i,j}| \leq 0.5$

2. $0.75\|\tilde{\mathbf{b}}_\mathbf{i}\|^2 \leq \|\mu_{i+1,i}\tilde{\mathbf{b}}_\mathbf{i} + \tilde{\mathbf{b}}_\mathbf{i+1}\|^2$

LLL Algorithm

$$\begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \mathbf{b}_1 & \mathbf{b}_2 & \mathbf{b}_3 & \cdots & \mathbf{b}_n \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix} = \begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \tilde{\mathbf{b}}_3 & \cdots & \tilde{\mathbf{b}}_n \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix} \begin{bmatrix} 1 & \leq \frac{1}{2} & \leq \frac{1}{2} & \cdots & \leq \frac{1}{2} \\ 0 & 1 & \leq \frac{1}{2} & \cdots & \leq \frac{1}{2} \\ \cdots & 0 & 1 & \cdots & \leq \frac{1}{2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

<u>An LLL-reduced basis has:</u>

1. All $|\mu_{i,j}| \leq 0.5$

2. $0.75\|\tilde{\mathbf{b}}_i\|^2 \leq \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$

LLL Algorithm

swap

$$\begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \mathbf{b}_1 & \mathbf{b}_2 & \mathbf{b}_3 & \cdots & \mathbf{b}_n \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix} = \begin{bmatrix} | & | & | & \cdots & | \\ | & | & | & \cdots & | \\ \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \tilde{\mathbf{b}}_3 & \cdots & \tilde{\mathbf{b}}_n \\ | & | & | & \cdots & | \\ | & | & | & \cdots & | \end{bmatrix} \begin{bmatrix} 1 & \leq ½ & \leq ½ & \cdots & \leq ½ \\ 0 & 1 & \leq ½ & \cdots & \leq ½ \\ \cdots & 0 & 1 & \cdots & \leq ½ \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

<u>An LLL-reduced basis has:</u>

1. All $|\mu_{i,j}| \leq 0.5$
2. $0.75\|\tilde{\mathbf{b}}_i\|^2 \leq \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$

LLL Algorithm

swap

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

<u>An LLL-reduced basis has:</u>

1. All $|\mu_{i,j}| \leq 0.5$

2. $0.75\|\tilde{\mathbf{b}}_i\|^2 \leq \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$

APPLICATION OF LLL: THE SUBSET SUM PROBLEM

Subset Sum Problem

a_i , T in $\mathbf{Z}_M$

a_i are chosen randomly

T is a sum of a random subset of the a_i

$a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n \qquad T$

Find a subset of a_i's

that sums to T (mod M)

Subset Sum Problem

a_i , T in $\mathbf{Z}_{49}$

a_i are chosen randomly

T is a sum of a random subset of the a_i

15 31 24 3 14 11

$15 + 31 + 14 = 11 \pmod{49}$

How Hard is Subset Sum?

a_i, T in $\mathbf{Z}_M$

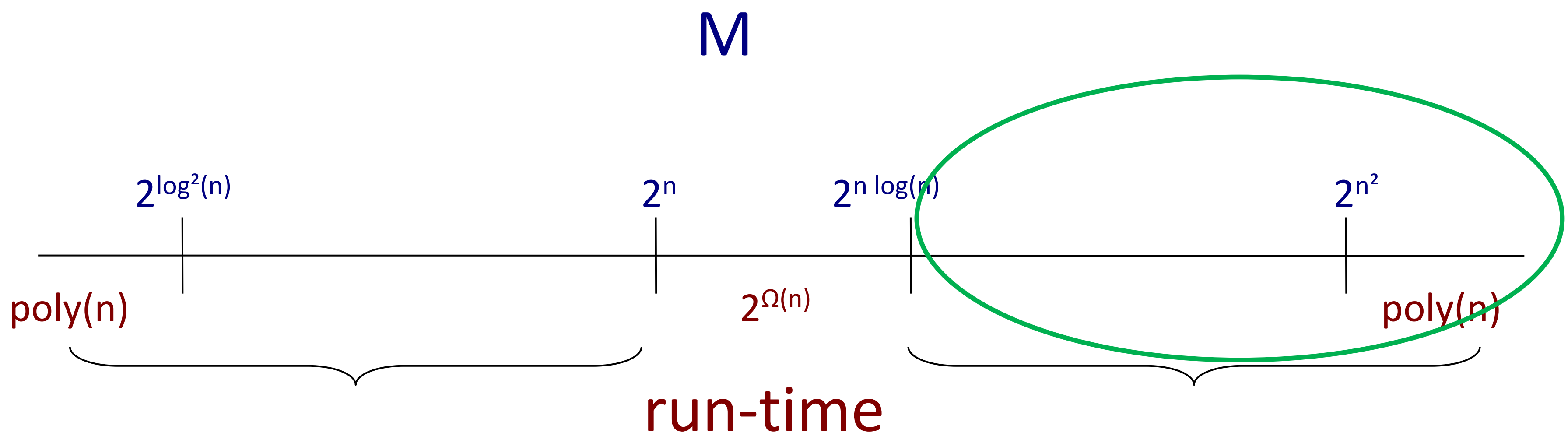
$a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n \qquad\qquad T$

Find a subset of a_i's that sums to T (mod M)

<u>Hardness Depends on</u>:

- Size of n and M
- Relationship between n and M

Complexity of Solving Subset Sum



"generalized birthday attacks"
[FlaPrz05,Lyu06,Sha08]

"lattice reduction attacks"
[LagOdl85,Fri86]

Subset Sum and Lattices

$a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n$ $\qquad T=(\Sigma a_i x_i \bmod M)$ for x_i in $\{0,1\}$

$\mathbf{a} = (a_1, a_2, \ldots , a_n, -T)$

$L^{\perp}(\mathbf{a}) = \{\mathbf{y} \text{ in } \mathbf{Z}^{n+1} : \mathbf{a}\cdot\mathbf{y} = 0 \bmod M\}$

Notice that $\mathbf{x}=(x_1, x_2, \ldots ,x_n,1)$ is in $L^{\perp}(\mathbf{a})$

$||\mathbf{x}|| < \sqrt{(n+1)}$

Want to use LLL to find this $\mathbf{x}$

When Will LLL Solve Subset Sum?

$L^{\perp}(\mathbf{a}) = \{\mathbf{y} \text{ in } \mathbf{Z}^{n+1} : \mathbf{a}\cdot\mathbf{y} = 0 \bmod M\}$

Notice that $\mathbf{x}=(x_1, x_2, \ldots, x_n, 1)$ is in $L^{\perp}(\mathbf{a})$, $\|\mathbf{x}\| < \sqrt{(n+1)}$

LLL can find a vector $< \delta^{n+1}\lambda_1(L^{\perp}(\mathbf{a})) < \delta^{n+1}\sqrt{(n+1)}$

So if there are *no other vectors* in $L^{\perp}(\mathbf{a})$ of length $< \delta^{n+1}\sqrt{(n+1)}$,
LLL must find $\mathbf{x}=(x_1, x_2, \ldots, x_n, 1)$!

Caveat: $\pm\mathbf{x}$, $\pm 2\mathbf{x}$, $\pm 3\mathbf{x}$, … are all in $L^{\perp}(\mathbf{a})$,
but we could recover $\mathbf{x}$ from these

Good vectors: $(kx_1, kx_2, \ldots, kx_n, k)$

The "Bad" Vectors

$\mathbf{y}=(y_1, \ldots ,y_n,k)$ such that $||\mathbf{y}||< \delta^{n+1} \sqrt{(n+1)} = r$

and

$$a_1y_1 + \ldots + a_ny_n - kT = 0 \bmod M$$

$$a_1y_1 + \ldots + a_ny_n - k(a_1x_1 + \ldots + a_nx_n) = 0 \bmod M$$

$$a_1(y_1 - kx_1) + \ldots + a_n(y_n - kx_n) = 0 \bmod M$$

(and for some i, $y_i - kx_i \neq 0 \bmod M$)

Probability of a Bad Lattice Vector

$S_r = \{ \mathbf{y} \text{ in } \mathbf{Z}^{n+1}, ||\mathbf{y}|| < r\}$

For any $(x_1,\ldots,x_n)$ in $\{0,1\}^n$ and $(y_1, \ldots ,y_n,k)$ in S_r :

$\Pr_{a_1, \ldots ,a_n}[a_1(y_1 - kx_1) + \ldots + a_n(y_n - kx_n) = 0 \bmod M]$

$= 1/M$ unless $(y_i - kx_i) = 0 \bmod M$ for all i

(the last line assumes that M is prime)

Probability of a Bad Lattice Vector

$S_r = \{ \mathbf{y} \text{ in } \mathbf{Z}^{n+1}, ||\mathbf{y}|| < r\}$

For <u>all</u> $(x_1,\ldots,x_n)$ in $\{0,1\}^n$ and $(y_1, \ldots ,y_n,k)$ in S_r such that $y_i - kx_i \neq 0 \bmod M$ for some i :

$$\Pr_{a_1, \ldots ,a_n}[a_1(y_1 - kx_1) + \ldots + a_n(y_n - kx_n) = 0 \bmod M]$$
$$\leq |S_r| \cdot 2^n / M$$

Want $|S_r| \cdot 2^n << M$

Number of $\mathbf{Z}^n$ Points in a Sphere

of integer points in a sphere of radius r

$\approx$

volume of sphere of radius r

$\approx$

$$(\pi n)^{-1/2}(2\pi e/n)^{n/2}\, r^n$$

(r needs to be at least $n^{1/2+\varepsilon}$)

Probability of a Bad Lattice Vector

Want $|S_r| \cdot 2^n << M$, where $r = \delta^{n+1} \sqrt{(n+1)}$

$$|S_r| \cdot 2^n < 9^{n+1} \cdot \delta^{(n+1)^2}$$

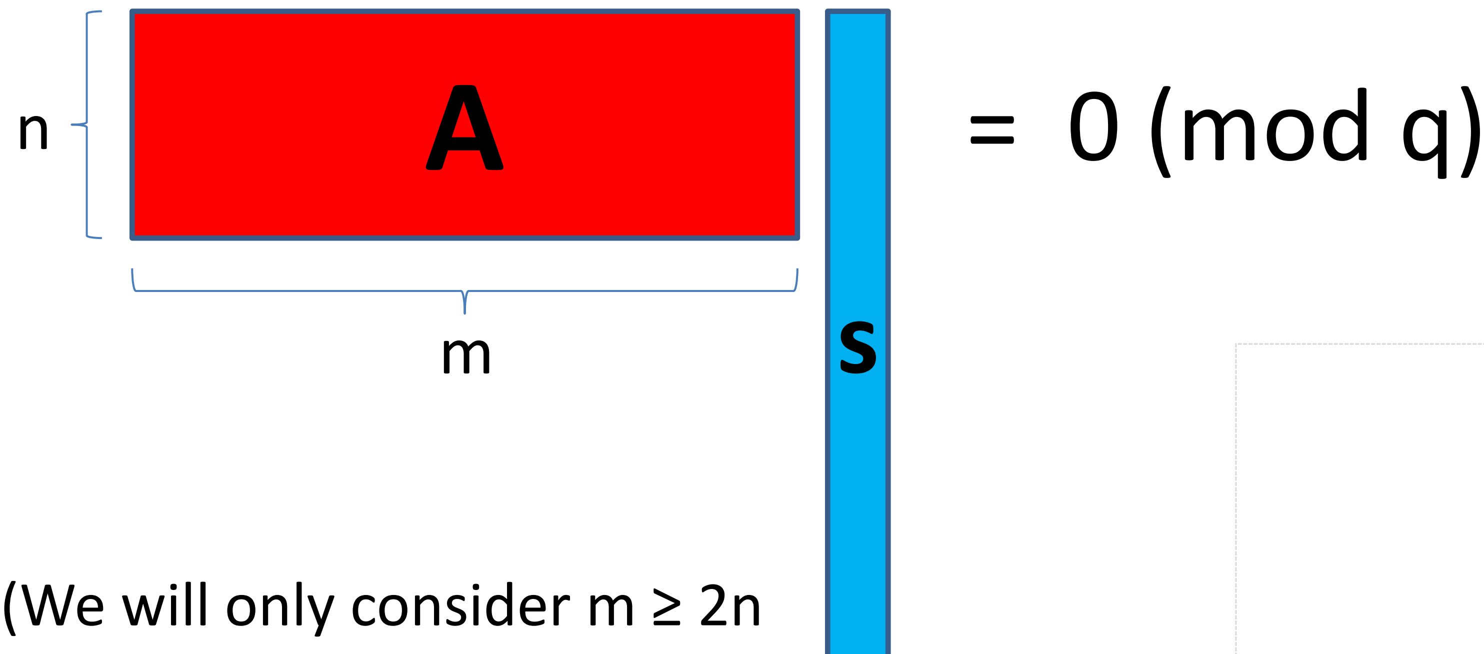
If $M > 9^{n+1} \cdot \delta^{(n+1)^2}$, subset sum can be solved in poly-time

(for all but a negligible number of instances)

APPLICATION OF LLL: THE SIS PROBLEM

The SIS Problem

Given a random **A** in $\mathbf{Z}_q^{n \times m}$,
Find a "small" **s** such that **As** = **0** mod q



(We will only consider m ≥ 2n and q > m)

Finding "Small" Vectors Using LLL

$L^{\perp}(\mathbf{A}) = \{\mathbf{y} \text{ in } \mathbf{Z}^m : \mathbf{Ay} = 0 \bmod q\}$

What is the shortest vector of $L^{\perp}(\mathbf{A})$?

Minkowski's Theorem: $\lambda_1(L^{\perp}(\mathbf{A})) \leq \sqrt{m}\, \det(L^{\perp}(\mathbf{A}))^{1/m}$

What is $\det(L^{\perp}(\mathbf{A}))^{1/m}$?

Determinant of an Integer Lattice

If L is an integer lattice, then det(L) = # ($\mathbf{Z}^m$/ L)

1. #($\mathbf{Z}^m$/ $L^\perp(\mathbf{A})$) $\leq q^n$

   For any $\mathbf{x}_1$, $\mathbf{x}_2$ in $\mathbf{Z}^m$, if $\mathbf{A}\mathbf{x}_1 = \mathbf{A}\mathbf{x}_2$ mod q, then $\mathbf{x}_1$, $\mathbf{x}_2$ are in the same coset of $\mathbf{Z}^m$/ $L^\perp(\mathbf{A})$.

2. If **A** has n linearly-independent columns, then #($\mathbf{Z}^m$/ $L^\perp(\mathbf{A})$) $= q^n$

   For every $\mathbf{y}$ in $\mathbf{Z}_q^n$, there is an $\mathbf{x}$ in $\mathbf{Z}^m$ such that $\mathbf{A}\mathbf{x}=\mathbf{y}$ mod q

Shortest Vector in $L^{\perp}(\mathbf{A})$

Minkowski's Theorem: $\lambda_1(L^{\perp}(\mathbf{A})) \leq \sqrt{m}\ \det(L^{\perp}(\mathbf{A}))^{1/m}$

For almost all $\mathbf{A}$, $\det(L^{\perp}(\mathbf{A})) = q^n$

Thus, $\lambda_1(L^{\perp}(\mathbf{A})) \leq \sqrt{m}\ q^{n/m}$

Can it be much smaller??

If $q^{n/m} \gg \sqrt{2\pi e}$, then No.

Shortest Vector in $L^{\perp}(\mathbf{A})$

$S_r = \{\, \mathbf{y} \text{ in } \mathbf{Z}^m, \|\mathbf{y}\| < r\}$

For any $\mathbf{s}\neq\mathbf{0}$ mod q in S_r, $\Pr_{\mathbf{A}}[\mathbf{As} = 0 \bmod q] = 1/q^n$

For all $\mathbf{s}\neq\mathbf{0}$ mod q in S_r, $\Pr_{\mathbf{A}}[\mathbf{As} = 0 \bmod q] \leq |S_r|/q^n$

$\approx (\pi m)^{-1/2}(2\pi e/m)^{m/2}\, r^m / q^n$

r needs to be $\approx \sqrt{m/(2\pi e)}\,q^{n/m}$

(since we assumed, $q^{n/m} >> \sqrt{2\pi e}$, we have $r >> \sqrt{m}$, and so
\# of integer points in a sphere of radius r ≈ volume of sphere of radius r)

Shortest Vector in $L^{\perp}(\mathbf{A})$

For almost all $\mathbf{A}$ in $\mathbf{Z}_q^{n \times m}$, when $q^{n/m} >> \sqrt{2\pi e}$

$$(1-\varepsilon)\sqrt{m/(2\pi e)}\,q^{n/m} \leq \lambda_1(L^{\perp}(\mathbf{A})) \leq \sqrt{m}\; q^{n/m}$$

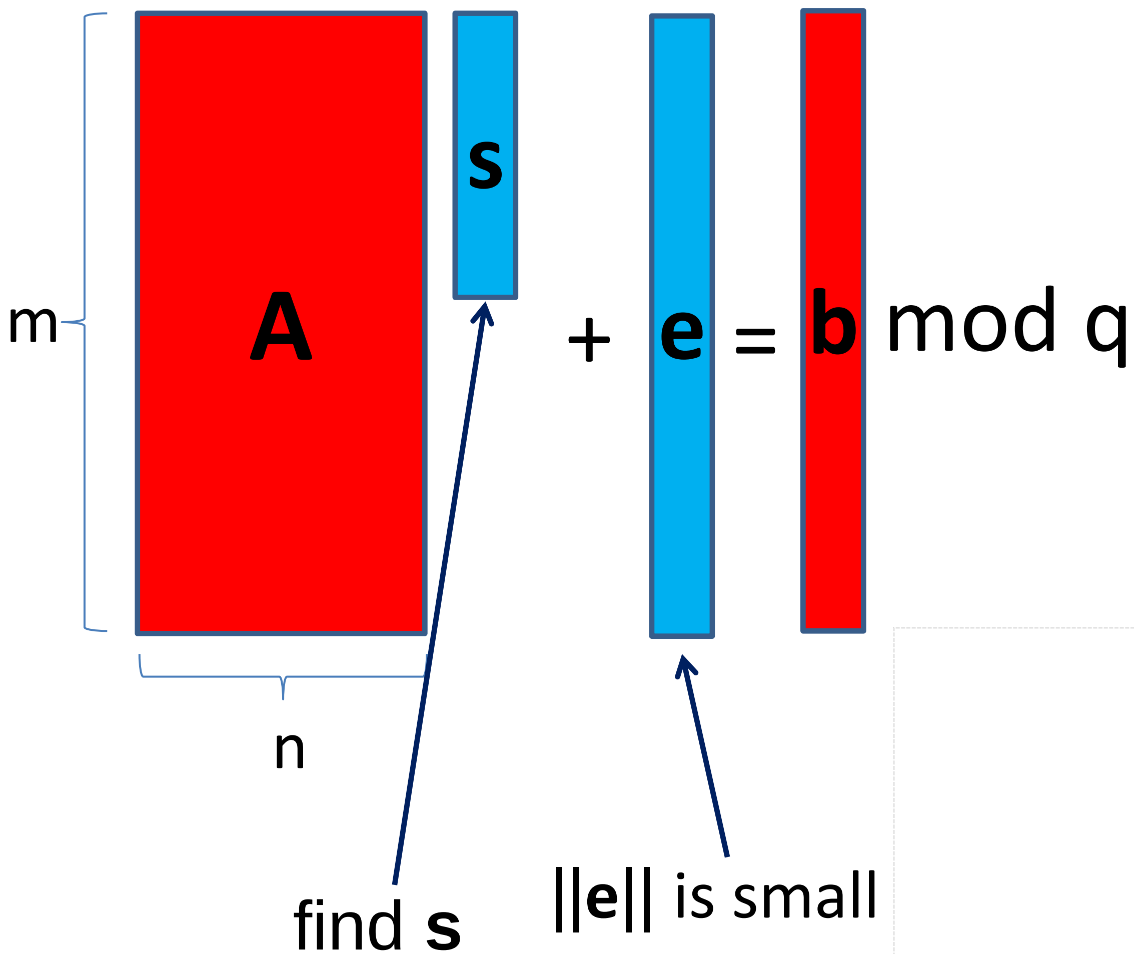
Experiments show that it's closer to this

Using LLL, can find a vector of length $\delta^m \cdot \sqrt{m/(2\pi e)}\,q^{n/m}$

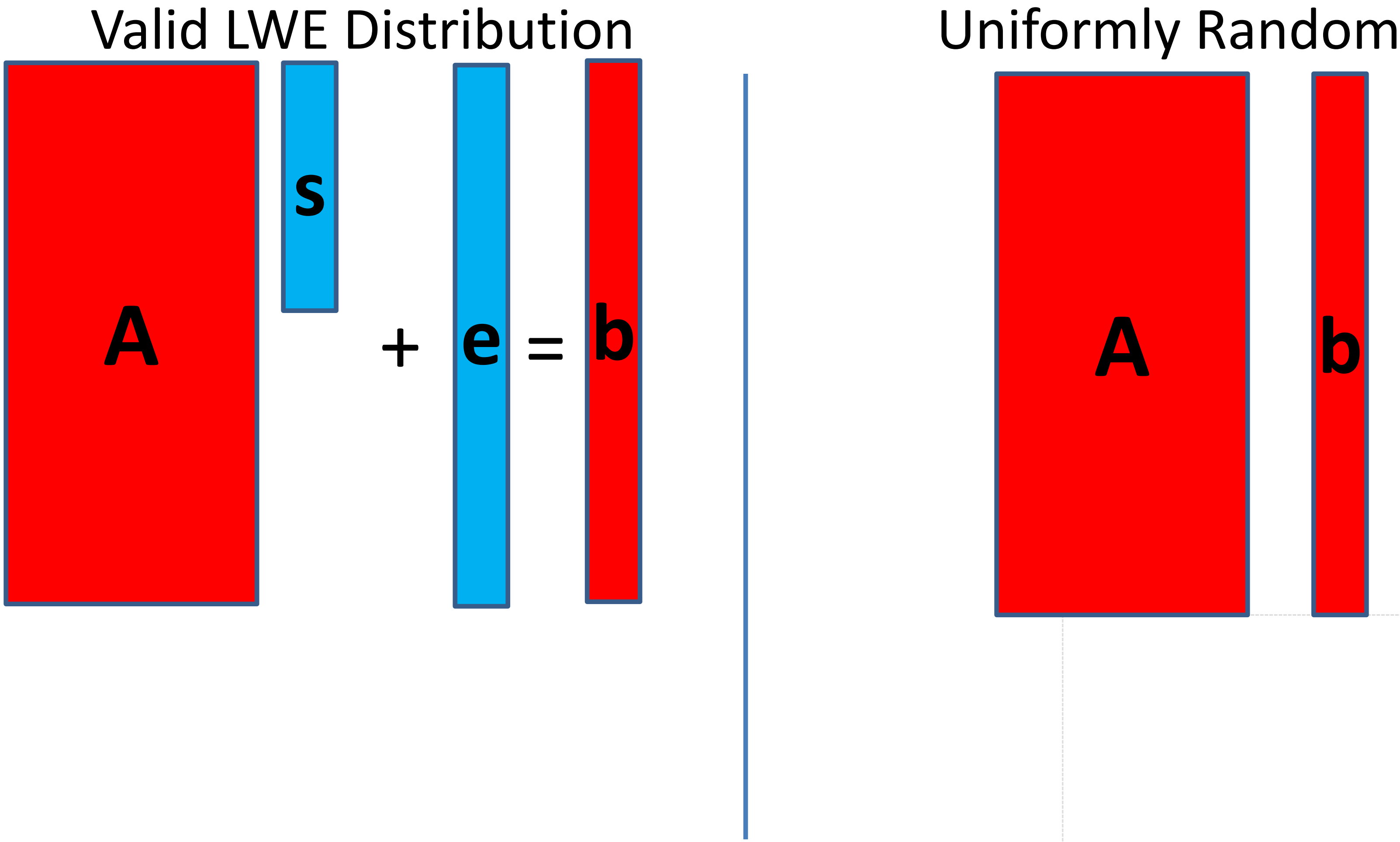
- Sometimes, to break a system, need to bound the infinity norm, so could be harder
- Sometimes it makes sense to not use all m columns

APPLICATION OF LLL: THE LWE PROBLEM

The LWE Problem

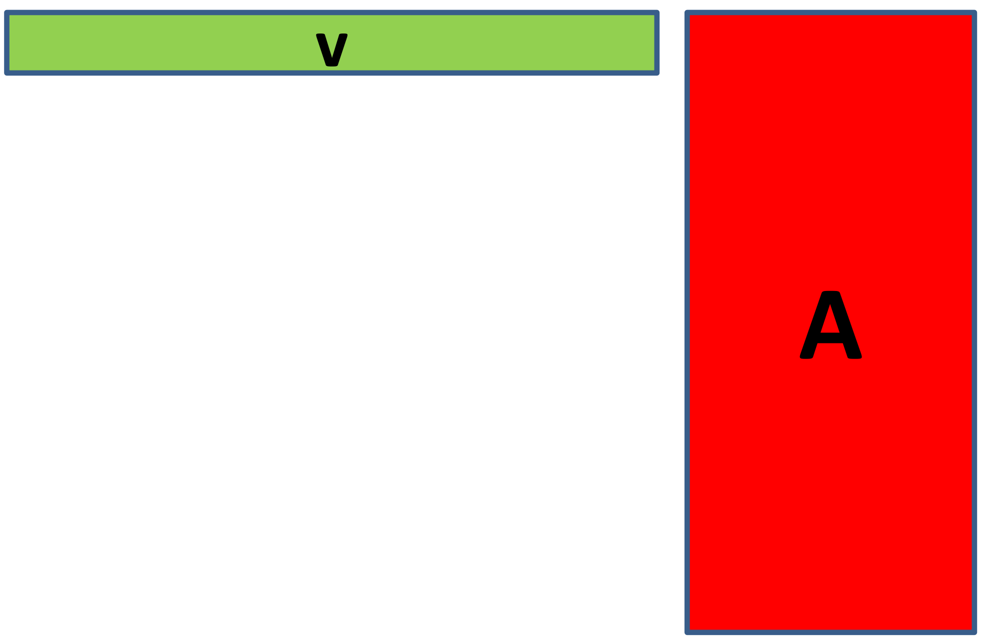


Decision LWE



Solve SIS to Solve LWE

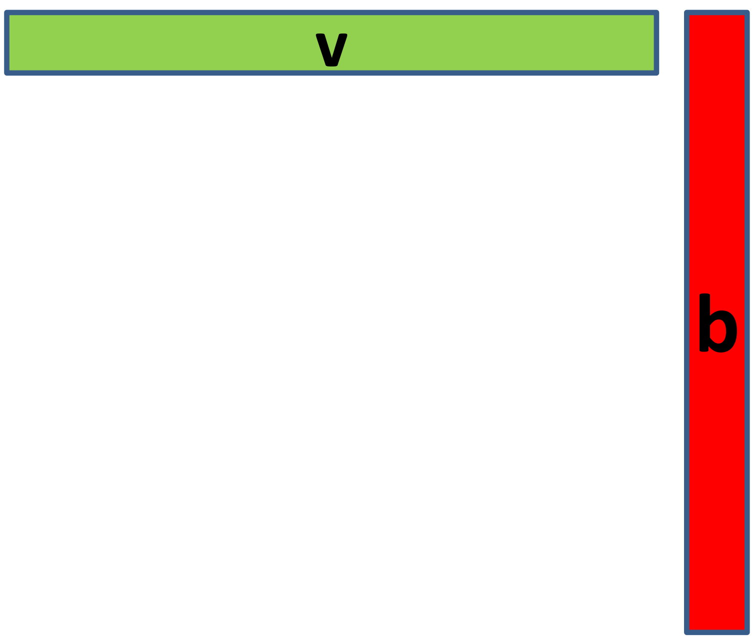
Using LLL, can find a vector **v** of length $\delta^m \cdot \sqrt{m/(2\pi e)}\, q^{n/m}$
(set m optimally, to minimize the length of **v**)



= **0** mod q

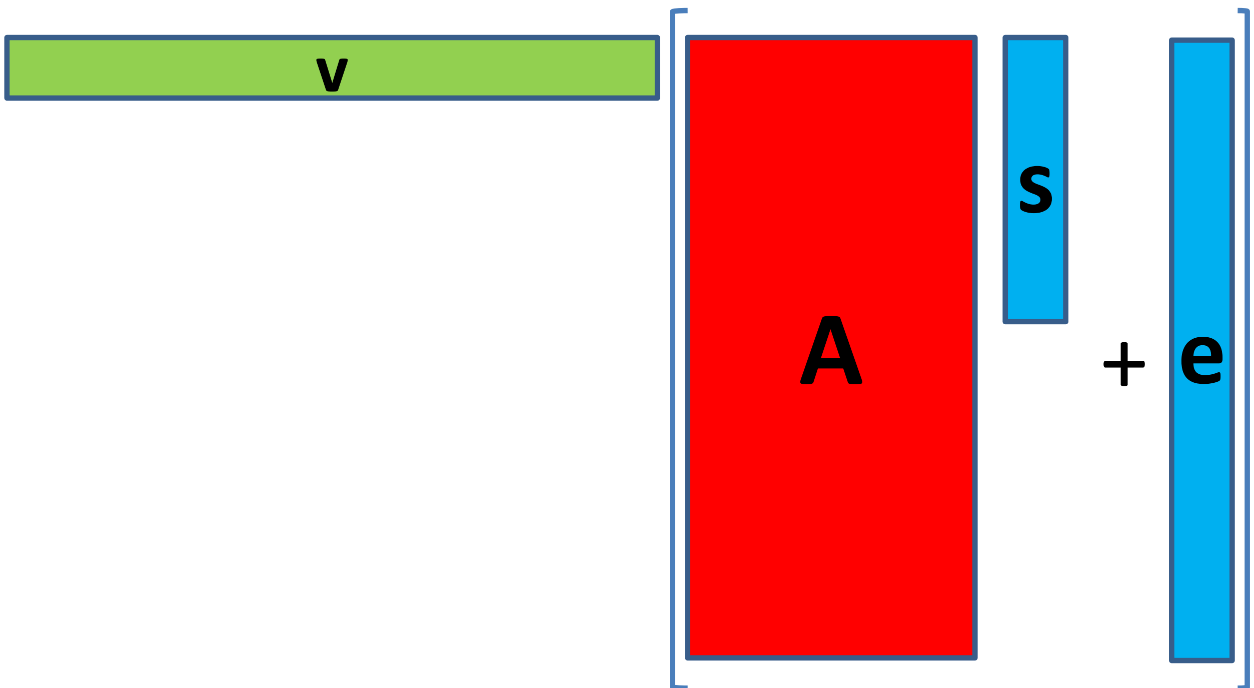
Solve SIS to Solve LWE

Using LLL, can find a vector **v** of length $\delta^m \cdot \sqrt{m/(2\pi e)}\, q^{n/m}$
(set m optimally, to minimize the length of **v**)
Compute **v**·**b** mod q.



Solve SIS to Solve LWE

Using LLL, can find a vector **v** of length $\delta^m \cdot \sqrt{m/(2\pi e)}\, q^{n/m}$
(set m optimally, to minimize the length of **v**)
Compute **v·b** mod q. If **b=As+e**, then **v·b** = **v·e** is small.



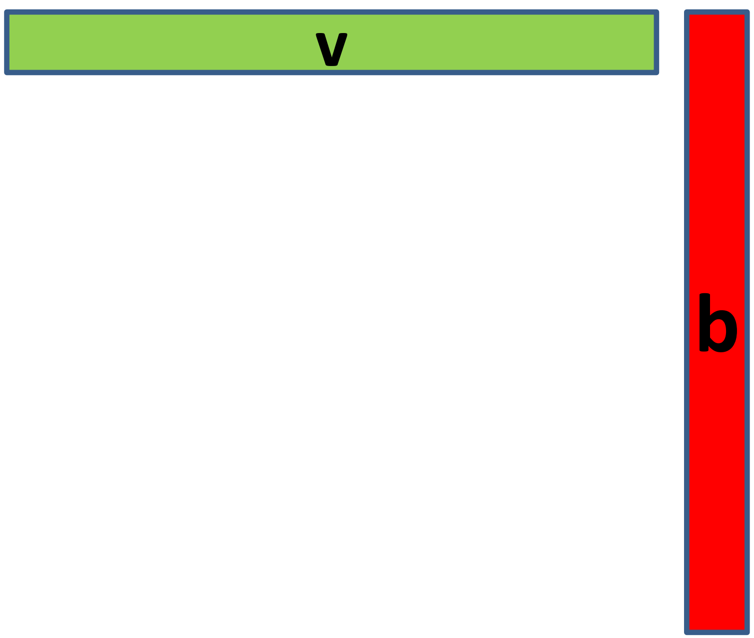
Solve SIS to Solve LWE

Using LLL, can find a vector **v** of length $\delta^m \cdot \sqrt{m/(2\pi e)}\,q^{n/m}$

(set m optimally, to minimize the length of **v**)

Compute **v·b** mod q. If **b=As+e**, then **v·b** = **v·e** is small.

If **b** is uniform, then **v·b** mod q is uniform.



Solve SIS to Solve LWE

Using LLL, can find a vector **v** of length $\delta^m \cdot \sqrt{m/(2\pi e)}\, q^{n/m}$
(set m optimally, to minimize the length of **v**)
Compute **v·b** mod q. If **b**=**As**+**e**, then **v·b** = **v·e** is small.
If **b** is uniform, then **v·b** mod q is uniform.

$\|\mathbf{v}\cdot\mathbf{e}\| \le \|\mathbf{v}\| \cdot \|\mathbf{e}\| \le \delta^m \cdot \sqrt{m/(2\pi e)}\, q^{n/m} \|\mathbf{e}\|$

So, if $\delta^m \cdot \sqrt{m/(2\pi e)}\, q^{n/m} \|\mathbf{e}\| < q/2$,
can solve decision LWE
and then search LWE as well

A Different Algorithm

- The previous algorithm assumed we could obtain a lot of samples. Many crypto applications do not provide this.

- If we don't have a lot of samples – can use "sample-preserving" reduction from search to decision LWE [MicMol '11]

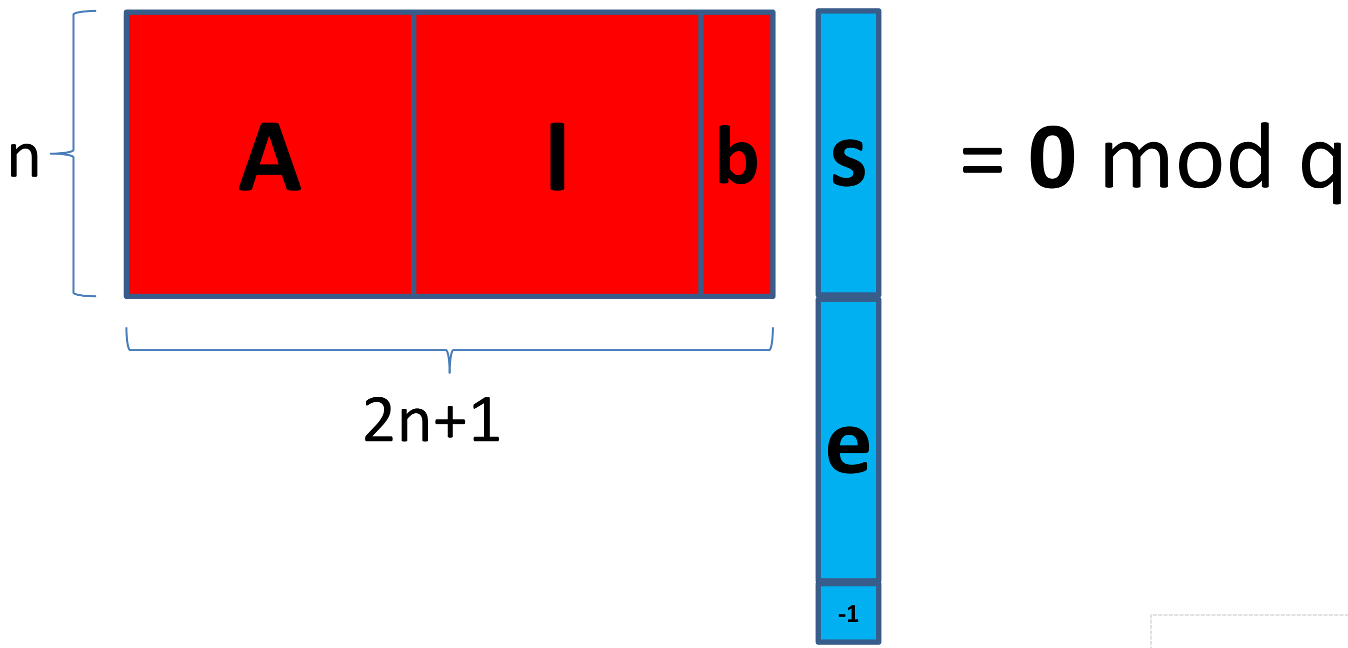
- In some cases, that reduction does not apply (e.g. ideal lattices …)

LWE Problem With Few Samples

$$n\left\{\underbrace{\mathbf{A}}_{n}\right. \; \mathbf{s} + \mathbf{e} = \mathbf{b} \mod q$$

$||\mathbf{e}||$ and $||\mathbf{s}||$ are small. find **s**.

LWE Problem With Few Samples



$L^{\perp}(\mathbf{A'})=\{\mathbf{y} \text{ in } \mathbf{Z}^{2n+1} : [\mathbf{A}|\mathbf{I}|\mathbf{b}]\mathbf{y} = 0 \bmod q\}$

Can show that for most **A**, the “bad” vectors have length at least $(1-\varepsilon)\sqrt{m/(2\pi e)}\,q^{n/m}$

Important Caveat

$L^{\perp}(\mathbf{A'})=\{\mathbf{y} \text{ in } \mathbf{Z}^{2n+1} : [\mathbf{A}|\mathbf{I}|\mathbf{b}]\mathbf{y} = 0 \bmod q\}$

Can show that for most **A**, the "bad" vectors have length at least $(1-\varepsilon)\sqrt{m/(2\pi e)}q^{n/m}$

Can find **s**,**e** if $\|\mathbf{s}|\mathbf{e}|\mathbf{-1}\| \leq \delta^m (1-\varepsilon)\sqrt{m/(2\pi e)}q^{n/m}$

What if LLL does not find **s,e**?

Then it will act as if the short vector **s|e|-1** does not exist!

IN PRACTICE

[Gama and Nguyen ‘08]

Two Types of Problems

Short Vector

given **A**, find a short **s** such that **As**=**0** mod q

||**s**|| is greater than $\det^{1/m}$

Unique Short Vector

given **A** and **As** mod q, find this short **s**

||**s**|| is less than $\det^{1/m}$

Unique Short Vector Problem

Looking for very short vector **s**

The next shortest vector not equal to k**s** is **v**

The hardness of finding **s** depends on ||**v**|| / ||**s**||

Let $\alpha = ||\mathbf{v}|| / ||\mathbf{s}|| = \lambda_2 / \lambda_1$

Short Vector Problem

Looking for vector **s** such that **As** = **0** mod q

(and there are no very short vectors in $L^{\perp}(\mathbf{A})$)

The shortest **s** that can be found depends on

$\alpha = ||\mathbf{s}|| \,/\, \det(L^{\perp}(\mathbf{A}))^{1/m}$

Two Types of Problems

- Short Vector

i.e. given **A**, find a short **s** such that **As**=**0** mod q

$\alpha = ||\mathbf{s}|| / \det(L^{\perp}(\mathbf{A}))^{1/m}$

- Unique Short Vector

i.e. given **A** and **As** mod q, find this short **s**

$\mathbf{A}' = [\mathbf{A} | \mathbf{As}]$

$\alpha = \lambda_2(L^{\perp}(\mathbf{A}')) / ||\mathbf{s}||$

$\approx \lambda_1(L^{\perp}(\mathbf{A})) / ||\mathbf{s}||$

$\alpha=1.02^m$	Can be broken using LLL
$\alpha=1.01^m$	Can be broken using BKZ (improvement of LLL)
$\alpha=1.007^m$	Seems quite secure for now
$\alpha=1.005^m$	Seems quite secure for the foreseeable future

Further References

LLL Algorithm: Oded Regev's lecture notes
www.cs.tau.ac.il/~odedr/teaching/lattices_fall_2009/index.html

Cryptanalysis using lattice reduction algorithms:

Nicolas Gama and Phong Nguyen: "Predicting Lattice Reduction"

Oded Regev and Daniele Micciancio: "Lattice-Based Cryptography"