# Introduction to lattice cryptography

**Damien Stehlé**

ENS Lyon

Edinburgh, July 2022

# Lattice-based cryptography

Probably the most mature approach for quantum-safe crypto.
Allows advanced cryptographic constructions
(homomorphic enc., some functional enc., privacy-preserving primitives, etc)

Topics covered in this introduction:

1. Hardness foundations: what are the assumptions?
2. Basic schemes: how to encrypt and sign?
3. More efficient schemes using algebraic lattices

References:

- C. Peikert: a decade of lattice-based cryptography
  eprint 2015/939
- V. Lyubashevsky: basic lattice cryptography
  on Lyubashevsky's webpage

# Lattice-based cryptography

Probably the most mature approach for quantum-safe crypto.
Allows advanced cryptographic constructions
(homomorphic enc., some functional enc., privacy-preserving primitives, etc)

Topics covered in this introduction:

1. Hardness foundations: what are the assumptions?
2. Basic schemes: how to encrypt and sign?
3. More efficient schemes using algebraic lattices

References:

- C. Peikert: a decade of lattice-based cryptography

  eprint 2015/939

- V. Lyubashevsky: basic lattice cryptography

  on Lyubashevsky's webpage

# Plan for this lecture

1. Background on Euclidean lattices.
2. The SIS and LWE problems.
3. Encrypting from LWE.

# Euclidean lattices

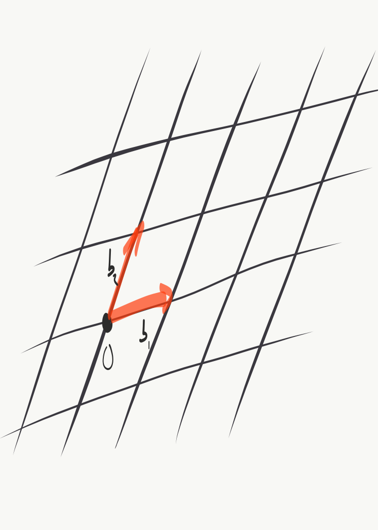
Lattice $\equiv$ discrete subgroup of $\mathbb{R}^n$

$$\equiv \quad \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$$

If the $\mathbf{b}_i$'s are linearly independent, they are called a **basis**.

Bases are not unique, but they can be obtained from each other by integer transforms of determinant $\pm 1$:

$$\begin{bmatrix} -2 & 1 \\ 10 & 6 \end{bmatrix} = \begin{bmatrix} 4 & -3 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$



# Euclidean lattices

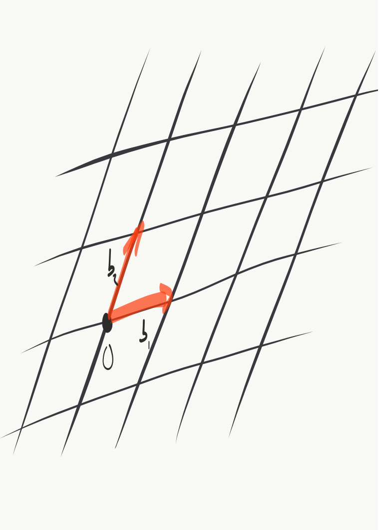
Lattice $\equiv$ discrete subgroup of $\mathbb{R}^n$

$$\equiv \quad \{\sum_{i \le n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$$

If the $\mathbf{b}_i$'s are linearly independent, they are called a **basis**.

Bases are not unique, but they can be obtained from each other by integer transforms of determinant $\pm 1$:

$$\begin{bmatrix} -2 & 1 \\ 10 & 6 \end{bmatrix} = \begin{bmatrix} 4 & -3 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$



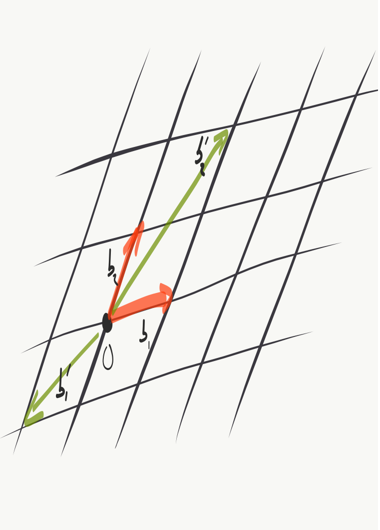
# Euclidean lattices

Lattice $\equiv$ discrete subgroup of $\mathbb{R}^n$
$\equiv \quad \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

If the $\mathbf{b}_i$'s are linearly independent, they are called a **basis**.

Bases are not unique, but they can be obtained from each other by integer transforms of determinant $\pm 1$:

$$\begin{bmatrix} -2 & 1 \\ 10 & 6 \end{bmatrix} = \begin{bmatrix} 4 & -3 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$



# Lattice invariants

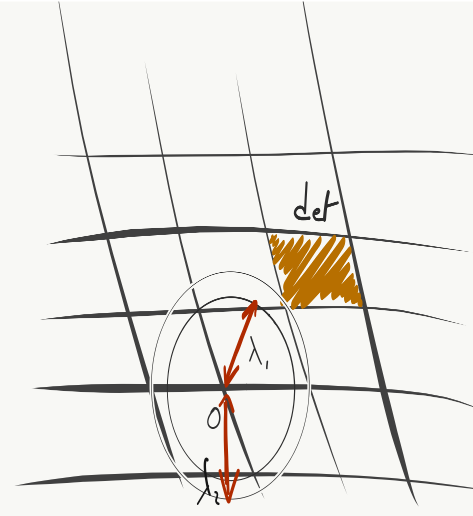
**Dimension**: $n$

**First minimum**:
$\lambda_1 = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$

**Last minimum**:
$\lambda_n = \min \{ r : \text{span}(L \cap \mathcal{B}(r)) = \text{span}(L) \}$

**Lattice determinant**:
$\det\ L = |\det(\mathbf{b}_i)_i|$, for any basis

**Minkowski theorem**:
$\lambda_1(L) \leq \sqrt{n} \cdot (\det\ L)^{1/n}$



# Lattice invariants

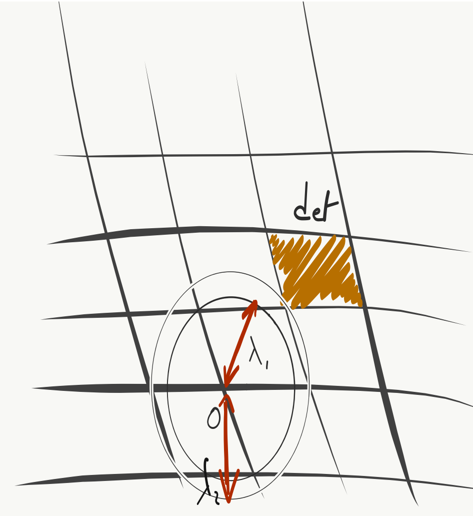
**Dimension**: $n$

**First minimum**:
$\lambda_1 = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$

**Last minimum**:
$$\lambda_n = \min\left\{ r : \operatorname{span}(L \cap \mathcal{B}(r)) = \operatorname{span}(L) \right\}$$

**Lattice determinant**:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis

**Minkowski theorem**:
$\lambda_1(L) \leq \sqrt{n} \cdot (\det L)^{1/n}$



# Lattice invariants

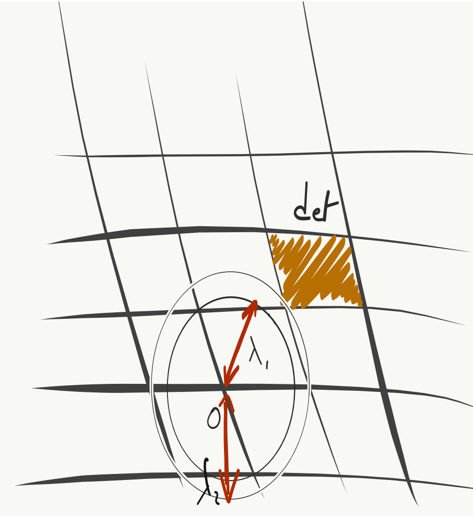
Dimension: $n$

First minimum:
$\lambda_1 = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$

Last minimum:
$\lambda_n = \min\{r : \operatorname{span}(L \cap \mathcal{B}(r)) = \operatorname{span}(L)\}$

Lattice determinant:
$\det\ L = |\det(\mathbf{b}_i)_i|$, for any basis

Minkowski theorem:
$\lambda_1(L) \leq \sqrt{n} \cdot (\det\ L)^{1/n}$



# Lattice invariants

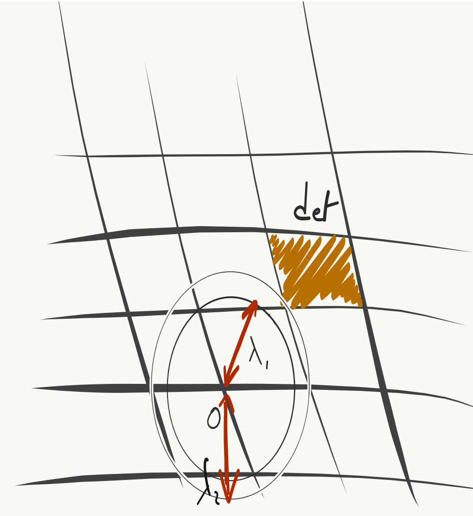
Dimension: $n$

First minimum:
$\lambda_1 = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$

Last minimum:
$\lambda_n = \min\left\{ r : \operatorname{span}(L \cap \mathcal{B}(r)) = \operatorname{span}(L) \right\}$

Lattice determinant:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis

Minkowski theorem:
$\lambda_1(L) \leq \sqrt{n} \cdot (\det L)^{1/n}$



# An example: construction A lattices

**Construction A.** Let $m \geq n \geq 1$ and $q \geq 2$ prime (for tranquility)

Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$. Then $L(\mathbf{A}) := \mathbf{A} \cdot \mathbb{Z}_q^n + q \cdot \mathbb{Z}^m$ is a lattice.

$\dim L(\mathbf{A}) = m$ & for full-rank $\mathbf{A}$: $\det L(\mathbf{A}) = q^{m-n}$

**SEE BOARD**

# An example: construction A lattices

**Construction A.** Let $m \geq n \geq 1$ and $q \geq 2$ prime (for tranquility)

Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$. Then $L(\mathbf{A}) := \mathbf{A} \cdot \mathbb{Z}_q^n + q \cdot \mathbb{Z}^m$ is a lattice.

$\dim L(\mathbf{A}) = m$ & for full-rank $\mathbf{A}$: $\det L(\mathbf{A}) = q^{m-n}$

By Minkowski, for full-rank $\mathbf{A}$: $\lambda_1(L(\mathbf{A})) \leq \min\left(\sqrt{m} q^{(m-n)/m}, q\right)$.

For $\mathbf{A}$ uniform, this is tight, up to a constant factor.

**SEE BOARD**

# Another example

Let $m \geq n \geq 1$ and $q \geq 2$ prime.

**Construction A for the orthogonal code**

Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$. Then $\mathbf{A}^\perp = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0}\ [q]\}$ is a lattice.

- Dimension: $m$
- Determinant: $q^{rk(\mathbf{A})}$.
- $\lambda_1 \approx \min(\sqrt{n \log q}, \sqrt{m} q^{n/m})$, with probability $\approx 1$ for a uniform $\mathbf{A}$.

# Another example

Let $m \geq n \geq 1$ and $q \geq 2$ prime.

**Construction A for the orthogonal code**

Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$. Then $\mathbf{A}^\perp = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \ [q]\}$ is a lattice.

- Dimension: $m$
- Determinant: $q^{rk(\mathbf{A})}$.
- $\lambda_1 \approx \min(\sqrt{n \log q}, \sqrt{m} q^{n/m})$, with probability $\approx 1$ for a uniform $\mathbf{A}$.

# SVP and SIVP

**The Shortest Vector Problem: SVP$_\gamma$**

Given a basis of $L$, find $\mathbf{b} \in L \setminus \mathbf{0}$ such that: $\|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

# SVP and SIVP

**The Shortest Vector Problem: $\mathrm{SVP}_\gamma$**

Given a basis of $L$, find $\mathbf{b} \in L \setminus \mathbf{0}$ such that: $\|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

**The Shortest Independent Vectors Problem: $\mathrm{SIVP}_\gamma$**

Given a basis of $L$, find $\mathbf{b}_1, \ldots, \mathbf{b}_n \in L$ lin. indep. such that:

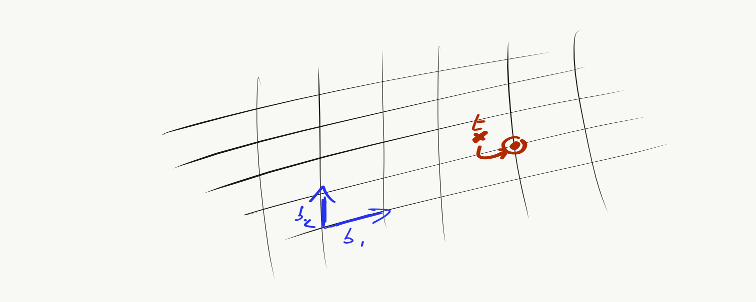
$$\max \|\mathbf{b}_i\| \leq \gamma \cdot \lambda_n(L).$$

# CVP and BDD

## The Closest Vector Problem: $\mathrm{CVP}_\gamma$

Given a basis of $L$ and a target $\mathbf{t} \in \mathbb{Q}^n$, find $\mathbf{b} \in L$ such that:

$$\|\mathbf{b} - \mathbf{t}\| \leq \gamma \cdot \min(\|\mathbf{c} - \mathbf{t}\| : \mathbf{c} \in L).$$




## $\mathrm{BDD}_\gamma$ (Bounded Distance Decoding)

Find the closest $\mathbf{b} \in L$ to $\mathbf{t}$, under the promise that $\|\mathbf{b} - \mathbf{t}\| \leq \lambda_1(L)/\gamma$.

# Hardness of SVP, SIVP, CVP, BDD

- NP-hard for some $\gamma = O(1)$ (under randomized reductions for SVP).
- Most of lattice crypto uses $\gamma = \mathcal{P}oly(n)$:
  for such $\gamma$, all known (quantum) algorithms cost $2^{\Omega(n)}$.
- Solvable in polynomial time when $\gamma = 2^{\widetilde{O}(n)}$.

**Major open problems**

- How equivalent are these problems? See survey by Noah Stephens-Davidowitz
- Can we beat the $2^{\Omega(n)}$ cost barrier?

But these are worst-case problems, which is not convenient for crypto.

# Hardness of SVP, SIVP, CVP, BDD

- NP-hard for some $\gamma = O(1)$ (under randomized reductions for SVP).
- Most of lattice crypto uses $\gamma = \mathcal{P}oly(n)$:
  for such $\gamma$, all known (quantum) algorithms cost $2^{\Omega(n)}$.
- Solvable in polynomial time when $\gamma = 2^{\widetilde{O}(n)}$.

**Major open problems**

- How equivalent are these problems? See survey by Noah Stephens-Davidowitz
- Can we beat the $2^{\Omega(n)}$ cost barrier?

But these are worst-case problems, which is not convenient for crypto.

# Plan for this lecture

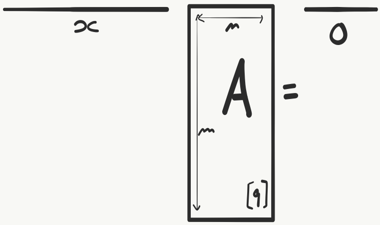
1. Background on Euclidean lattices.
2. **The SIS and LWE problems.**
3. Encrypting from LWE.

# $\mathsf{SIS}_{\beta,q,m}$ [Ajtai'96]

**The Short Integer Solution Problem**

Given a uniform $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m$ such that:

$$0 < \|\mathbf{x}\| \leq \beta \quad \text{and} \quad \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \bmod q.$$



# SIS as a lattice problem

Remember our lattice example:

$$\mathbf{A}^{\perp} = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0}\ [q]\}.$$

SIS consists in finding a short non-zero vector in $\mathbf{A}^{\perp}$, for a uniform $\mathbf{A}$.

- If $\beta < \lambda_1 \approx \min(\sqrt{n \log q}, \sqrt{m} q^{n/m})$: trivially hard.
- If $\beta \geq q$: trivially easy.
- In between: interesting.

**SIS is an average-case SVP/SIVP.**

# SIS as a lattice problem

Remember our lattice example:

$$\mathbf{A}^\perp = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0}\ [q]\}.$$

SIS consists in finding a short non-zero vector in $\mathbf{A}^\perp$, for a uniform $\mathbf{A}$.

- If $\beta < \lambda_1 \approx \min(\sqrt{n \log q}, \sqrt{m} q^{n/m})$: trivially hard.
- If $\beta \geq q$: trivially easy.
- In between: interesting.

**SIS is an average-case SVP/SIVP.**

# Hardness of SIS? [Ajtai96,...,GPV08]

**Worst-case to average-case reduction** $(\gamma \approx n\beta,\ q \geq \sqrt{n}\beta)$

Any efficient $\mathrm{SIS}_{\beta,q,m}$ algorithm succeeding with non-negligible probability leads to an efficient $\mathrm{SIVP}_\gamma$ algorithm.

**SKETCH: SEE BOARD**

# $\mathrm{LWE}_{\alpha,q}$ [Regev'05]

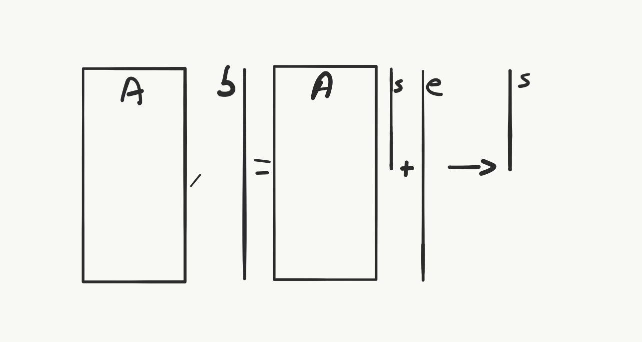
Let $\mathbf{s} \in \mathbb{Z}_q^n$. Let $D_{\mathbf{s},\alpha}$ be the distribution corresponding to:

$$(\mathbf{a}; \langle \mathbf{a}, \mathbf{s} \rangle + e \ [q]) \quad \text{with} \quad \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n), \ e \hookleftarrow \lfloor \nu_{\alpha q} \rceil,$$

where $\nu_{\alpha q}$ denotes the continuous Gaussian of st. dev. $\alpha q$.

**The Learning With Errors Problem — Search-$\mathrm{LWE}_\alpha$**

Let $\mathbf{s} \in \mathbb{Z}_q^n$. Given arbitrarily many samples from $D_{\mathbf{s},\alpha}$, find $\mathbf{s}$.



# LWE as a lattice problem

**Search-LWE$_\alpha$**

Let $\mathbf{s} \in \mathbb{Z}_q^n$. Given $(\mathbf{A}; \mathbf{A}\mathbf{s} + \mathbf{e}\ [q])$ with $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ and $\mathbf{e} \hookleftarrow \lfloor \nu_{\alpha q}^m \rceil$ for and arbitrary $m$, find $\mathbf{s}$.

Remember our lattice example $L_{\mathbf{A}} = \mathbf{A} \cdot \mathbb{Z}_q^n + q \cdot \mathbb{Z}^m$.

- If $\alpha \approx 0$, then LWE is easy to solve.
- If $\alpha \gg 1$, then LWE is trivially hard.
- In between: interesting.

**LWE is an average-case BDD.**

# LWE as a lattice problem

**Search-LWE$_\alpha$**

Let $\mathbf{s} \in \mathbb{Z}_q^n$. Given $(\mathbf{A}; \mathbf{A}\mathbf{s} + \mathbf{e}\ [q])$ with $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ and $\mathbf{e} \hookleftarrow \lfloor \nu_{\alpha q}^m \rceil$ for and arbitrary $m$, find $\mathbf{s}$.

Remember our lattice example $L_{\mathbf{A}} = \mathbf{A} \cdot \mathbb{Z}_q^n + q \cdot \mathbb{Z}^m$.

- If $\alpha \approx 0$, then LWE is easy to solve.
- If $\alpha \gg 1$, then LWE is trivially hard.
- In between: interesting.

**LWE is an average-case BDD.**

# How hard is LWE? [Regev05]

**Quantum worst-case to average-case reduction** $(\gamma \approx n/\alpha,\ \alpha q \geq \sqrt{n})$

Assume that $q$ is prime and $\mathcal{P}oly(n)$.
Any efficient $\mathrm{LWE}_{n,\alpha,q}$ algorithm succeeding with non-negligible probability leads to an efficient **quantum** $\mathrm{SIVP}_\gamma$ algorithm.

# How hard is LWE? [Regev05]

**Quantum worst-case to average-case reduction** $(\gamma \approx n/\alpha,\ \alpha q \geq \sqrt{n})$

Assume that $q$ is prime and $\mathcal{P}oly(n)$.
Any efficient $\mathrm{LWE}_{n,\alpha,q}$ algorithm succeeding with non-negligible probability leads to an efficient **quantum** $\mathrm{SIVP}_\gamma$ algorithm.

# How hard is LWE? [Regev05]

**Quantum worst-case to average-case reduction** $(\gamma \approx n/\alpha,\ \alpha q \geq \sqrt{n})$

Assume that $q$ is prime and $\mathcal{P}oly(n)$.
Any efficient $\mathrm{LWE}_{n,\alpha,q}$ algorithm succeeding with non-negligible probability leads to an efficient **quantum** $\mathrm{SIVP}_\gamma$ algorithm.

- [Peikert09]: classical reduction, for $q \approx 2^n$, from BDD.
- [SSTX09]: simpler (but weaker) quantum reduction, from SIS.
- [BLPRS13]: de-quantized reduction, for any $q$ that is at least some $\mathcal{P}oly(n)$, from a weaker worst-case lattice problem.
- [BKSW18]: yet another quantum reduction, from BDD.

# Decision LWE

$$D_{\mathbf{s},\alpha}: \quad (\mathbf{a}; \langle \mathbf{a}, \mathbf{s} \rangle + e\ [q]) \quad \text{with} \quad \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n),\ e \hookleftarrow \lfloor \nu_{\alpha q} \rceil.$$

**Search-LWE$_\alpha$**

Let $\mathbf{s} \in \mathbb{Z}_q^n$. Given arbitrarily many samples from $D_{\mathbf{s},\alpha}$, find $\mathbf{s}$.

**Dec-LWE$_\alpha$**

Let $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$. With non-negligible probability over $\mathbf{s}$, distinguish between an oracle access to $D_{\mathbf{s},\alpha}$ or an oracle access to $U(\mathbb{Z}_q^{n+1})$.

# Decision LWE

$$D_{\mathbf{s},\alpha}: \quad (\mathbf{a}; \langle \mathbf{a}, \mathbf{s}\rangle + e\ [q]) \quad \text{with} \quad \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n),\ e \hookleftarrow \lfloor \nu_{\alpha q} \rceil.$$

**Search-LWE$_\alpha$**

Let $\mathbf{s} \in \mathbb{Z}_q^n$. Given arbitrarily many samples from $D_{\mathbf{s},\alpha}$, find $\mathbf{s}$.

**Dec-LWE$_\alpha$**

Let $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$. With non-negligible probability over $\mathbf{s}$, distinguish between an oracle access to $D_{\mathbf{s},\alpha}$ or an oracle access to $U(\mathbb{Z}_q^{n+1})$.

# Decision LWE

$$D_{\mathbf{s},\alpha}: \quad (\mathbf{a}; \langle \mathbf{a}, \mathbf{s} \rangle + e\ [q]) \quad \text{with} \quad \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n),\ e \hookleftarrow \lfloor \nu_{\alpha q} \rceil.$$

**Search-LWE$_\alpha$**

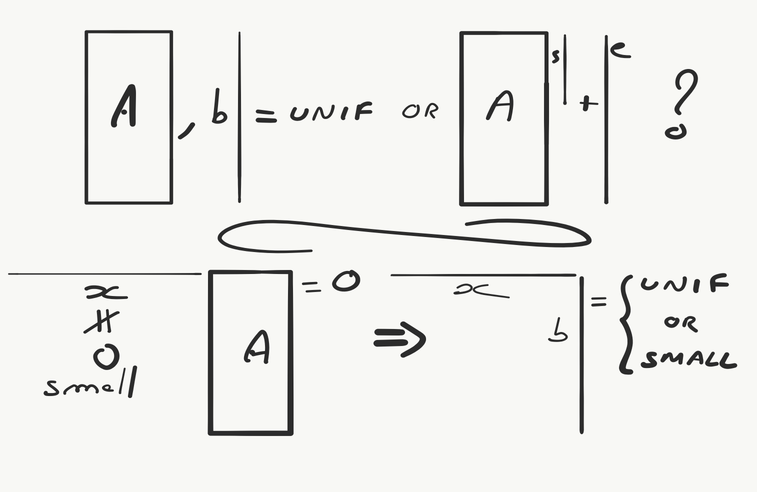
Let $\mathbf{s} \in \mathbb{Z}_q^n$. Given arbitrarily many samples from $D_{\mathbf{s},\alpha}$, find $\mathbf{s}$.

**Dec-LWE$_\alpha$**

Let $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$. With non-negligible probability over $\mathbf{s}$, distinguish between an oracle access to $D_{\mathbf{s},\alpha}$ or an oracle access to $U(\mathbb{Z}_q^{n+1})$.

Dec-LWE and Search-LWE efficiently reduce to one another.

# Decision LWE and SIS



# Nice properties of LWE

1. Arbitrary number of samples
   $\Rightarrow$ can amplify success probability and distinguishing advantage.
2. Random self-reducibility
   $\Rightarrow$ solving for a non-negligible fraction of $\mathbf{s}$'s suffices.

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) + (\mathbf{0}, \mathbf{A} \cdot \mathbf{t}) = (\mathbf{A}, \mathbf{A} \cdot (\mathbf{s} + \mathbf{t}) + \mathbf{e})$$

3. A distinguishing oracle allows to check a guess for a coordinate of $\mathbf{s}$.

$\Rightarrow$ These lead to a search-to-decision reduction.

4. Can take different types of noises:
   - Discrete Gaussian
   - Uniform integer in an interval
   - Deterministic, using rounding

# Nice properties of LWE

1. Arbitrary number of samples
   $\Rightarrow$ can amplify success probability and distinguishing advantage.
2. Random self-reducibility
   $\Rightarrow$ solving for a non-negligible fraction of $\mathbf{s}$'s suffices.

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) + (\mathbf{0}, \mathbf{A} \cdot \mathbf{t}) = (\mathbf{A}, \mathbf{A} \cdot (\mathbf{s} + \mathbf{t}) + \mathbf{e})$$

3. A distinguishing oracle allows to check a guess for a coordinate of $\mathbf{s}$.

$\Rightarrow$ These lead to a search-to-decision reduction.

4. Can take different types of noises:
   - Discrete Gaussian
   - Uniform integer in an interval
   - Deterministic, using rounding

# Nice properties of LWE

1. Arbitrary number of samples
   $\Rightarrow$ can amplify success probability and distinguishing advantage.
2. Random self-reducibility
   $\Rightarrow$ solving for a non-negligible fraction of $\mathbf{s}$'s suffices.

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) + (\mathbf{0}, \mathbf{A} \cdot \mathbf{t}) = (\mathbf{A}, \mathbf{A} \cdot (\mathbf{s} + \mathbf{t}) + \mathbf{e})$$

3. A distinguishing oracle allows to check a guess for a coordinate of $\mathbf{s}$.

$\Rightarrow$ These lead to a search-to-decision reduction.

4. Can take different types of noises:
   - Discrete Gaussian
   - Uniform integer in an interval
   - Deterministic, using rounding

# Nice properties of LWE

1. Arbitrary number of samples
   $\Rightarrow$ can amplify success probability and distinguishing advantage.
2. Random self-reducibility
   $\Rightarrow$ solving for a non-negligible fraction of $\mathbf{s}$'s suffices.

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e}) + (\mathbf{0}, \mathbf{A} \cdot \mathbf{t}) = (\mathbf{A}, \mathbf{A} \cdot (\mathbf{s} + \mathbf{t}) + \mathbf{e})$$

3. A distinguishing oracle allows to check a guess for a coordinate of $\mathbf{s}$.

$\Rightarrow$ These lead to a search-to-decision reduction.

4. Can take different types of noises:
   - Discrete Gaussian
   - Uniform integer in an interval
   - Deterministic, using rounding

# Open problems

## Selected problems on SIS/LWE

- Can we get hardness of SIS/LWE based on SIVP with approximation factor less than $n$?
- Can we reduce $\mathrm{SVP}_\gamma$ to SIS/LWE?
- Can we get a classical reduction from SIVP to LWE with parameters equivalent to those of Regev's quantum reduction?
- Or is this discrepancy intrinsic and there is a quantum acceleration for solving LWE and SIVP?

# Open problems

## Selected problems on SIS/LWE

- Can we get hardness of SIS/LWE based on SIVP with approximation factor less than $n$?
- Can we reduce $\mathrm{SVP}_\gamma$ to SIS/LWE?
- Can we get a classical reduction from SIVP to LWE with parameters equivalent to those of Regev's quantum reduction?
- Or is this discrepancy intrinsic and there is a quantum acceleration for solving LWE and SIVP?

# Open problems

## Selected problems on SIS/LWE

- Can we get hardness of SIS/LWE based on SIVP with approximation factor less than $n$?
- Can we reduce $\mathrm{SVP}_\gamma$ to SIS/LWE?
- Can we get a classical reduction from SIVP to LWE with parameters equivalent to those of Regev's quantum reduction?
- Or is this discrepancy intrinsic and there is a quantum acceleration for solving LWE and SIVP?

# Plan for this lecture

1. Background on Euclidean lattices.
2. The SIS and LWE problems.
3. **Encrypting from LWE.**

SVP/SIVP/CVP/BDD are here only implicitly:
(almost) no need to know lattices to design lattice-based schemes!

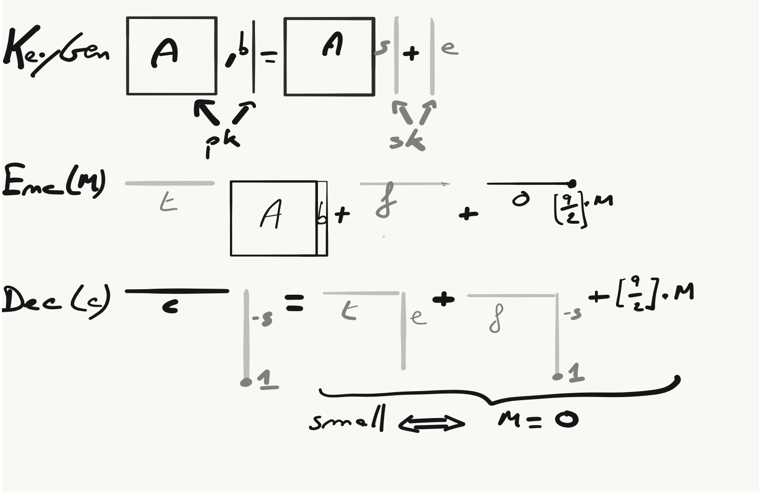
# LWE with small secret [ACPS09]

**Small-secret-LWE$_\alpha$**

Let $\mathbf{s} \hookleftarrow \lfloor \nu_{\alpha q} \rceil^n$. With non-negligible probability over $\mathbf{s}$, distinguish between (arbitrarily many) samples from $D_{\mathbf{s},\alpha}$ or from $U(\mathbb{Z}_q^{n+1})$.

**SEE BOARD**

# LWE-based encryption [LPS10]



# Decryption correctness

To ensure correctness, it suffices that

$$\left| \mathbf{t}^T \mathbf{e} + \mathbf{f}^T (-\mathbf{s}|1) \right| \ < \ q/4,$$

with probability very close to 1.

Up to the roundings of Gaussians:

- Gaussian tail bound $\Rightarrow$ $\|\mathbf{t}\|, \|\mathbf{e}\|, \|\mathbf{f}\|, \|\mathbf{s}\| \lesssim \sqrt{n}\alpha q$ with probability $1 - 2^{-\Omega(n)}$.
- It suffices that $(\sqrt{n}\alpha q)^2 \lesssim q/4$, i.e., $\alpha \lesssim 1/(n\sqrt{q})$.

# Decryption correctness

To ensure correctness, it suffices that

$$\left|\mathbf{t}^T\mathbf{e} + \mathbf{f}^T(-\mathbf{s}|1)\right| \; < \; q/4,$$

with probability very close to 1.

Up to the roundings of Gaussians:

- Gaussian tail bound $\Rightarrow$ $\|\mathbf{t}\|, \|\mathbf{e}\|, \|\mathbf{f}\|, \|\mathbf{s}\| \lesssim \sqrt{n}\alpha q$ with probability $1 - 2^{-\Omega(n)}$.
- It suffices that $(\sqrt{n}\alpha q)^2 \lesssim q/4$, i.e., $\alpha \lesssim 1/(n\sqrt{q})$.

# Passive security (IND-CPA)

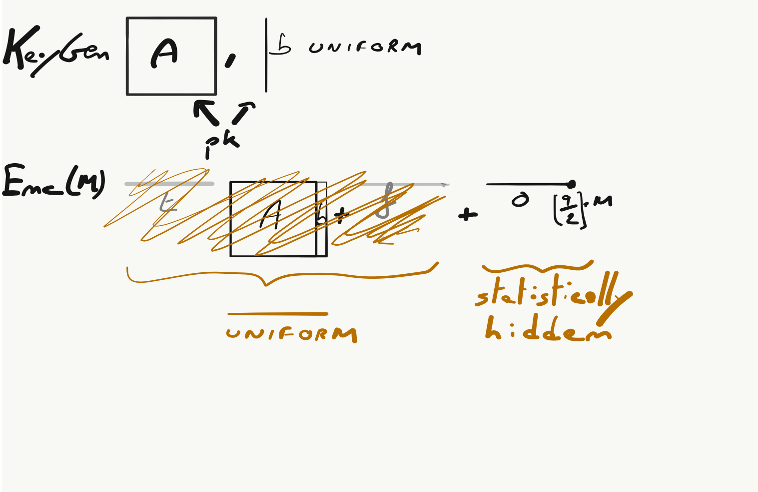
KeyGen $\boxed{A}$ , $b = \cancel{\boxed{A}\, s + e}$ | $b$ UNIFORM

pk

sk

Enc($M$) $t$ $\boxed{A \mid b}$ + $f$ + $0$ $\lfloor \frac{q}{2} \rceil \cdot M$

# Passive security (IND-CPA)



# Setting parameters (asymptotically)

How do we choose $n$, $\alpha$ and $q$?

Minimize bandwidth/key-size/run-times under the conditions that:

- Correctness holds
- Some security is guaranteed

Take $\sqrt{n}/q \approx 1/(n\sqrt{q})$, i.e., $q \approx n^3$.

Take $\alpha \approx \sqrt{n}/q \approx n^{-5/2}$.

(Don't use the SIVP to LWE reduction to set concrete parameters!)

# Setting parameters (asymptotically)

How do we choose $n$, $\alpha$ and $q$?

Minimize bandwidth/key-size/run-times under the conditions that:

- Correctness holds
- Some security is guaranteed

Take $\sqrt{n}/q \approx 1/(n\sqrt{q})$, i.e., $q \approx n^3$.

Take $\alpha \approx \sqrt{n}/q \approx n^{-5/2}$.

(Don't use the SIVP to LWE reduction to set concrete parameters!)

# Setting parameters (asymptotically)

How do we choose $n$, $\alpha$ and $q$?

Minimize bandwidth/key-size/run-times under the conditions that:

- Correctness holds $\alpha \lesssim 1/(n\sqrt{q})$
- Some security is guaranteed $\alpha q \geq \sqrt{n}$

Take $\sqrt{n}/q \approx 1/(n\sqrt{q})$, i.e., $q \approx n^3$.

Take $\alpha \approx \sqrt{n}/q \approx n^{-5/2}$.

(Don't use the SIVP to LWE reduction to set concrete parameters!)

# Setting parameters (asymptotically)

How do we choose $n$, $\alpha$ and $q$?

Minimize bandwidth/key-size/run-times under the conditions that:

- Correctness holds $\alpha \lesssim 1/(n\sqrt{q})$
- Some security is guaranteed $\alpha q \geq \sqrt{n}$

Take $\sqrt{n}/q \approx 1/(n\sqrt{q})$, i.e., $q \approx n^3$.

Take $\alpha \approx \sqrt{n}/q \approx n^{-5/2}$.

(Don't use the SIVP to LWE reduction to set concrete parameters!)

# Open problems

## Selected problems on LWE encryption

- Do the diverse noise distributions have an impact?
- What is the best way to upgrade security from passive (CPA) to active (CCA)?

# Open problems

## Selected problems on LWE encryption

- Do the diverse noise distributions have an impact?
- What is the best way to upgrade security from passive (CPA) to active (CCA)?