Overview of Lattice based Cryptography
from Geometric Intuition to Basic Primitives

Léo Ducas
CWI, Amsterdam, The Netherlands

Spring School on Lattice-Based Cryptography
Oxford, March 2017
Content of the talk

- Geometric intuition behind lattice-based crypto
- The modern formalism (SIS-LWE)
- Basic construction and difficulties
Outline

1 The Geometric point of view

2 The SIS-LWE Framework

3 Encryption is easy

4 Signatures are tricky
Definition

A lattice $L$ is a discrete subgroup of a finite-dimensional Euclidean vector space.
Bases of a Lattice

Good Basis $\mathbf{G}$ of $L$  
Bad Basis $\mathbf{B}$ of $L$

$\mathbf{G} \rightarrow \mathbf{B}$ : easy (randomization);
$\mathbf{B} \rightarrow \mathbf{G}$ : hard (LLL, BKZ, Lattice Sieve...).
An important invariant: the Volume

For any two bases $G, B$ of the same lattice $\Lambda$:

$$\det(GG^t) = \det(BB^t).$$

We can therefore define:

$$\text{vol}(\Lambda) = \sqrt{\det(GG^t)}.$$

Geometrically: the volume of any fundamental domain of $\Lambda$. 
An important invariant: the Volume

For any two bases \( G, B \) of the same lattice \( \Lambda \):

\[
\det(GG^t) = \det(BB^t).
\]

We can therefore define:

\[
\text{vol}(\Lambda) = \sqrt{\det(GG^t)}.
\]

Geometrically: the volume of any fundamental domain of \( \Lambda \).

Let \( G^* \) be the Gram-Schmidt Orthogonalization of \( G \)

\( G^* \) is not a basis of \( \Lambda \), nevertheless:

\[
\text{vol}(\Lambda) = \sqrt{\det(G^*G^{*t})} = \prod \|g_i^*\|.
\]
What is a “Good” basis

Recall that, independently of the basis $G$ it hold that:

$$\text{vol}(\Lambda) = \prod \|g_i^*\|.$$

Therefore, it is somehow equivalent that

- $\max_i \|g_i^*\|$ is small
- $\min_i \|g_i^*\|$ is large
- $\kappa(G) = \min_i \|g_i^*\| / \max_i \|g_i^*\|$ is small
What is a “Good” basis

Recall that, independently of the basis $G$ it hold that:

$$\text{vol}(\Lambda) = \prod \|g_i^*\|.$$ 

Therefore, it is somehow equivalent that

- $\max_i \|g_i^*\|$ is small
- $\min_i \|g_i^*\|$ is large
- $\kappa(G) = \min_i \|g_i^*\| / \max_i \|g_i^*\|$ is small

Good basis (rule of thumb)

$$\kappa(G) = \text{poly}(d), \quad \forall i, \|g_i^*\| = \text{poly}(d) \cdot \text{vol}(\Lambda)^{1/d}.$$
What is a “Good” basis

Recall that, independently of the basis $G$ it hold that:

$$\text{vol}(\Lambda) = \prod \|g_i^*\|.$$ 

Therefore, it is somehow equivalent that

- $\max_i \|g_i^*\|$ is small
- $\min_i \|g_i^*\|$ is large
- $\kappa(G) = \min_i \|g_i^*\| / \max_i \|g_i^*\|$ is small

**Good basis (rule of thumb)**

$$\kappa(G) = \text{poly}(d), \quad \forall i, \|g_i^*\| = \text{poly}(d) \cdot \text{vol}(\Lambda)^{1/d}.$$ 

**LLL-reduced basis (rule of thumb)**

$$\kappa(G) \approx (1.04)^d, \quad \max_i \|g_i^*\| \approx (1.02)^d \cdot \text{vol}(\Lambda)^{1/d}.$$
Each basis defines a **parallelepipedic tiling**.

**Round’off Algorithm [Lenstra, Babai]:**
Bases and Fundamental Domains

Each basis defines a **parallelepipedic tiling**.

**Round’off Algorithm** [Lenstra, Babai]:
- Given a target \( t \)
Bases and Fundamental Domains

Each basis defines a parallelepipedic tiling.

Round’off Algorithm [Lenstra, Babai]:

- Given a target $t$
- Find’s $v \in L$ at the center the tile.
Round’off Algorithm

ROUND OFF Algorithm [Lenstra, Babai]:

Use $B$ to switch to the lattice $\mathbb{Z}^n$ ($\times B - 1$)
round each coordinate (square tiling)
switch back to $L$ ($\times B$)

$t' = B - 1 \cdot t$
$v' = \lfloor t' \rfloor$
$v = B \cdot v'$
Round’off Algorithm

**RoundOff Algorithm** [Lenstra, Babai]:
- Use \( \mathbf{B} \) to switch to the lattice \( \mathbb{Z}^n (\times \mathbf{B}^{-1}) \)

\[
t' = \mathbf{B}^{-1} \cdot t;
\]
Round’off Algorithm

**RoundOff Algorithm** [Lenstra, Babai]:

- Use $B$ to switch to the lattice $\mathbb{Z}^n (\times B^{-1})$
- round each coordinate (square tiling)

$t' = B^{-1} \cdot t$; $v' = \lfloor t' \rfloor$
Round’off Algorithm

**RoundOff Algorithm** [Lenstra, Babai]:

- Use $B$ to switch to the lattice $\mathbb{Z}^n \times B^{-1}$
- Round each coordinate (square tiling)
- Switch back to $L \times B$

$$t' = B^{-1} \cdot t; \quad v' = \lfloor t' \rfloor; \quad v = B \cdot v'$$
There is a better algorithm ($\text{NearestPlane}$) based on Gram-Schmidt Orth. $B^*$ of a basis $B$:

- **Worst-case distance:** $\frac{1}{2} \sqrt{\sum \|b_i^*\|^2}$ (Approx-CVP)
- **Correct decoding of** $t = v + e$ where $v \in \Lambda$ if $\|e\| \leq \min \|b_i^*\|$ (BDD)
With a good basis $G$ one can solve Approx-CVP / BDD. Given only a bad basis $B$, solving CVP is a hard problem.

Can this somehow be used as a trapdoor?
Using the (second) decoding algorithm, one can recover \(v, e\) from \(w = v + e\) when

\[\|e\| \leq \min \|b_i^*\|\]

Fix a parameter \(\eta\):

- Private key: good basis \(G\) such that \(\|g_i^*\| \geq \eta\)
- Public key: bad basis \(B\) such that \(\|b_i^*\| \ll \eta\)
- Message : \(m \in \Lambda = \mathcal{L}(B) = \mathcal{L}(G)\)
- Ciphertext : \(c = m + e\), for a random error \(e\), \(\|e\| \leq \eta\)
- Decryption : \((m', e) = \text{NearestPlane}(c)\)
Encryption from lattices

Decryption: \((m', e) = \text{decode}(c)\)

- With the good basis \(G\), \(m' = m\)
- With the bad basis \(B\), \(m' \neq m\): decryption fails!

Léo Ducas, CWI, Amsterdam, The Netherlands
Signatures

**Sign**

- Hash the message to a random vector $m$.
- apply `NearestPlane` with a good basis $G$:
  find $s \in L$ close to $m$.

**Verify**

- check that $s \in L$ using the bad basis $B$
- and that $m$ is close to $s$.

Correct signature (close) Incorrect signature (far)

Léo Ducas, CWI, Amsterdam, The Netherlands  
Overview of Lattice based Cryptography
A statistical attack [NguReg06, DucNgu12]

The difference $s - m$ is always inside the parallelepiped spanned by the good basis $G$ (or its GSO $G^*$):

Each signatures $(s, m)$ leaks a bit of information about $G$.

**Learning a parallelepiped** from few signatures [Nguyen Regev 2006]:

⇒ Total break of original GGH and NTRUSign schemes.
Randomize the previous algorithms (Gaussian-sampling): the distribution $s - m$ can be made independent of $G$

- [Klein 2000, Gentry Peikert Vaikuthanathan 2008]: Slow and memory heavy, even in the ring-setting (NTRU, Ring-LWE)

- [Peikert 2010] Faster and less memory, but worse quality

- [D. Prest 15] (Fast Fourier Orthogonalization) Fast and good quality for certain rings
Outline

1. The Geometric point of view
2. The SIS-LWE Framework
3. Encryption is easy
4. Signatures are tricky
Let $q$ be a prime\(^1\) integer, and $n < m$ two positive integers. The matrix $\mathbf{A} \in \mathbb{Z}^{m \times n}_q$ spans the $q$-ary lattice:

$$\Lambda_q(\mathbf{A}) := \{ \mathbf{x} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}_q^n, \mathbf{x} \equiv \mathbf{A}\mathbf{y} \mod q \} = \mathbf{A} \cdot \mathbb{Z}_q^n + q\mathbb{Z}^m$$

### Lattice parameters

Assuming $\mathbf{A}$ is full-rank:

- $\text{dim}(\Lambda_q(\mathbf{A})) = m$
- $\text{vol}(\Lambda_q(\mathbf{A})) = q^{m-n}$

\(^1\)Not necessarily, but simpler.
Let $q$ be a prime\(^2\) integer, and $n < m$ two positive integers. The matrix $A^t \in \mathbb{Z}_q^{n \times m}$ is the parity-check of the lattice:

$$\Lambda_q^{\perp}(A^t) := \{ x \in \mathbb{Z}^m | A^t x \equiv 0 \mod q \} = \ker(x \mapsto A^t x \mod q)$$

### Lattice parameters

Assuming $A$ is full-rank:

- $\dim(A) = m$
- $\text{vol}(A) = q^n$

---

\(^2\)Not necessarily, but simpler.
The Short Integer Solution Problem (SIS)

Definition (SIS assumption)
Given a random matrix $A$
Finding a small non-zero $x \in \mathbb{Z}_q^n$ such that $Ax \equiv 0 \mod q$ is hard.
The Short Integer Solution Problem (SIS)

**Definition (SIS assumption)**

Given a random matrix $A$
Finding a small non-zero $x \in \mathbb{Z}_q^n$ such that $Ax \equiv 0 \mod q$ is hard.

**Lattice formulation**

Solving Approx-SVP in $\Lambda_q^\perp(A^t)$ is hard.

Worst-case to average case connection due to [Ajtai 1998].
Set $S = \{0, 1\}^m$ and consider the function:

$$f_A : S \rightarrow \mathbb{Z}_q^n, \quad x \mapsto A^t x \mod q$$

**SIS $\Rightarrow$ Collision Resistant Hashing and One-Way Function**

- Finding collision\(^3\) is as hard as SIS (take the difference)

Moreover, if $m \gg n \log q$:

- $f_A$ is highly surjective (many pre-images exists)
- Finding pre-images is hard.

\(^3\)Collision must exist whenever $m > n \log_2 q$
The Learning With Error problem (LWE)

Let $\chi$ be a distribution of small errors $\ll q$.

**Definition (Decisional LWE)**

For $A \leftarrow \mathbb{Z}_{q}^{m \times n}$, $s \leftarrow \mathbb{Z}_{q}^{n}$, $e \leftarrow \chi^{m}$, distinguishing $(A, As + e)$ from uniform is hard.

**Definition (Search LWE)**

For $A \leftarrow \mathbb{Z}_{q}^{m \times n}$, $s \leftarrow \mathbb{Z}_{q}^{n}$, $e \leftarrow \chi^{m}$, given $(A, As + e)$, finding $s$ is hard.

Both problems are easily proved equivalent.
The Learning With Error problem (LWE)

Let \( \chi \) be a distribution of small errors \( \ll q \).

**Definition (Decisional LWE)**

For \( A \leftarrow \mathbb{Z}_{q}^{m \times n}, s \leftarrow \mathbb{Z}_{q}^{n}, e \leftarrow \chi^{m} \), distinguishing \((A, As + e)\) from uniform is hard.

**Definition (Search LWE)**

For \( A \leftarrow \mathbb{Z}_{q}^{m \times n}, s \leftarrow \mathbb{Z}_{q}^{n}, e \leftarrow \chi^{m} \), given \((A, As + e)\), finding \(s\) is hard.

Both problems are easily proved equivalent.

**Lattice formulation**

Solving BDD in \( \Lambda_{q}(A) \) is hard.

Worst-case to average case connection due to [Regev 2005].
LWE as unique-SVP (The embedding technique)

Given \((A, b = As + e)\), consider

\[ \Lambda = \Lambda_q(A, b) \]

Then:

- \(e \in \Lambda\), and \(\|e\| \approx \sigma \sqrt{m} \)
- one would expect \(\lambda_1(\Lambda) \approx \sqrt{\frac{m}{2\pi e}} \cdot q^{1-n/m} \)

Alternative lattice formulation

Solving Unique-SVP in \(\Lambda_q(A, b)\) is hard.
Simple application of LWE

Set \( S = \{-\sigma, \ldots, \sigma\}^m \) and consider the function:

\[
g_A : \mathbb{Z}_q^n \times S \rightarrow \mathbb{Z}_q^m, \quad (s, e) \mapsto As + e \mod q
\]

LWE \Rightarrow Secret-Key Encryption

Idea: Noisy one-time pad

- \( Enc_s(m \in \{0, 1\}) = (a, a^t s + e + \lfloor \frac{q}{2} \rfloor m) \)
- \( Dec_s(a, b) = \lfloor \frac{2}{q} (b - a^t s) \rfloor \mod 2 \)
Outline

1. The Geometric point of view
2. The SIS-LWE Framework
3. Encryption is easy
4. Signatures are tricky
Encryption is easy

Idea:

- Use one short lattice vector (rather than a full good basis $B$)
- This short vector is easy to hide: LWE as unique-SVP
Public Key Encryption, [Regev 2005]

\[ m \gg n \log q. \]

- \( SK = s \in \mathbb{Z}_q^m \)
- \( PK = (A; b = As + e) \in \mathbb{Z}_q^{(n+1) \times m} \)
- \( Enc(m) = (t^T \cdot A, t^T \cdot b + \lceil \frac{q}{2} \rceil m + e) \), where \( t \leftarrow \{0, 1\}^{n+1} \)
- \( Dec(x^t, y) \) Compute

\[
d = y - x^t s = t^t e + e + \left\lfloor \frac{q}{2} \right\rfloor m
\]

and return \( m = \left\lfloor \frac{2}{q} d \right\rfloor \mod 2 \)
Public Key Encryption, [Regev 2005]

\[ m \gg n \log q. \]

- \[ SK = s \in \mathbb{Z}_q^m \]
- \[ PK = (A; b = As + e) \in \mathbb{Z}_q^{(n+1) \times m} \]
- \[ Enc(m) = (t^t \cdot A, t^t \cdot b + \lfloor \frac{q}{2} \rfloor m + e), \text{ where } t \leftarrow \{0, 1\}^{n+1} \]
- \[ Dec(x^t, y) \text{ Compute} \]

\[ d = y - x^t s = t^t e + e + \lfloor \frac{q}{2} \rfloor m \]

and return \[ m = \lfloor \frac{2}{q} d \rfloor \mod 2 \]

Proof sketch for CPA security

- Replace PK by uniform random \((A, b)\)
- Apply the left-over hash lemma on \(t\) over \((A, b)\)
- \(Enc(m)\) is statistically close to uniform.
Using a Systematic-Normal form, one can assume that \( s \leftarrow \chi^n \) is small as well. Take \( m = n \).

- \( PK = s \in \mathbb{Z}_q^n \)
- \( SK = (A; b = As + e) \in \mathbb{Z}_q^{(n+1) \times n} \)
- \( Enc(m) = (A^t s' + e', b^t s' + e' + e + \lfloor \frac{q}{2} \rfloor m) \)
- \( Dec(x, y) : Compute \)

\[
d = y - x^t s = s^t e' + s'^t e + e + \lfloor \frac{q}{2} \rfloor m
\]

and return \( m = \lfloor \frac{2}{q} d \rfloor \mod 2 \)
Using a Systematic-Normal form, one can assume that \( s \leftarrow \chi^n \) is small as well. Take \( m = n \).

- \( PK = s \in \mathbb{Z}_q^n \)
- \( SK = (A; b = As + e) \in \mathbb{Z}_{(n+1) \times n} \)
- \( Enc(m) = (A^t s' + e', b^t s' + e' + e + \lfloor \frac{q}{2} \rfloor m) \)
- \( Dec(x, y) \): Compute
  \[
d = y - x^t s = s^t e' + s'^t e + e + \lfloor \frac{q}{2} \rfloor m
\]
  and return \( m = \lfloor \frac{2}{q} d \rfloor \mod 2 \)

**Proof sketch for CPA security**

- Replace PK by uniform random by LWE assumption
- Replace \( Enc(m) \) by uniform random by LWE assumption

Can also be made an approximate key Exchange.
Are the above CCA-secure?

NO!

It is Additively Homomorphic therefore can’t be CCA2. CCA1 attacks left as an exercise.\textsuperscript{4}

Generic Transform to CCA security in the Random Oracle Model?
Chosen-Ciphertext Secure?

Are the above CCA-secure?

**NO!**

It is Additively Homomorphic therefore can’t be CCA2. CCA1 attacks left as an exercise.⁴

Generic Transform to CCA security in the Random Oracle Model?

**Yes [Peikert 2013]**

Correctness needs to hold with overwhelming probability.

---

⁴ Toy with the error and see if Dec. fails
Chosen-Ciphertext Secure?

Are the above CCA-secure?

**NO!**

It is Additively Homomorphic therefore can’t be CCA2. CCA1 attacks left as an exercise.\(^4\)

Generic Transform to CCA security in the Random Oracle Model?

**Yes [Peikert 2013]**

Correctness needs to hold with overwhelming probability.

And in the plain Model?

**Yes**

But costly: requires Trapdoors (e.g [Micciancio Peikert 2012])

Open question: Cramer-Shoup for lattices?

\(^4\) Toy with the error and see if Dec. fails
Outline

1. The Geometric point of view
2. The SIS-LWE Framework
3. Encryption is easy
4. Signatures are tricky
Solution 1: Hash-Then-Sign

Sign
- Hash the message to a random vector \( m \).
- apply \textsc{GaussianSampling} with a good basis \( G \):
  
    find \( s \in L \) close to \( m \).

Verify
- check that \( s \in L \) using the bad basis \( B \)
- and that \( m \) is close to \( s \).
Definition (The Matrix-NTRU assumption)

For two small matrices $F, G \leftarrow \mathcal{X}^{n \times n}$, set $H = FG^{-1} \mod q$. Distinguishing $H$ from uniform is hard.\(^5\)

---

\(^5\) $H$ is provably uniform for midly large $F, G$ [Stehle Steinfeld 2012]

\(^6\) IMHO: Precise parameter proposal not conservative enough
Definition (The Matrix-NTRU assumption)

For two small matrices $F, G \leftarrow \chi^{n \times n}$, set $H = FG^{-1} \mod q$. Distinguishing $H$ from uniform is hard.$^5$

Do not overstretched!

Can be much weaker than (Ring) LWE for large $q$.
cf. Thursday : [A. Bai D. 2016, Kirchner Fouque 2016]

---

$^5$ $H$ is provably uniform for midly large $F, G$ [Stehle Steinfeld 2012]

$^6$ IMHO: Precise parameter proposal not conservative enough
Definition (The Matrix-NTRU assumption)

For two small matrices $F, G \leftarrow \chi^{n \times n}$, set $H = FG^{-1} \mod q$.
Distinguishing $H$ from uniform is hard.$^5$

Do not overstretched!

Can be much weaker than (Ring) LWE for large $q$.

cf. Thursday: [A. Bai D. 2016, Kirchner Fouque 2016]

- $(F, G)$ is a good partial basis of the lattice.
- It can be completed into a full good basis.
  - optimal parameters studied in [D. Prest Lyubashevski 2013]$^6$

---

$^5$ $H$ is provably uniform for midly large $F, G$ [Stehle Steinfeld 2012]

$^6$ IMHO: Precise parameter proposal not conservative enough
SoA: [Micciancio Peikert 2012] “Simpler, Tighter, Faster, Smaller”.

- Define a Gadget matrix \( \mathbf{G} = [\mathbf{I}, 2\mathbf{I}, 4\mathbf{I}, \ldots 2^k \mathbf{I}] \)
- Start from a truly random matrix \( \mathbf{A} \)
- Extend \( \mathbf{A} \) to \( \mathbf{A'} = [\mathbf{A} | \mathbf{RA} + \mathbf{G}] \) for a small matrix \( \mathbf{R} \)
- \( \mathbf{A'} \) is statistically uniform (leftover hash lemma)
- \( \mathbf{R} \) provides a good basis of \( \Lambda^\bot(\mathbf{A}) \)

+ Many extensions (tags, basis delegation)
+ Very convenient for advanced crypto
- Cumbersome for basic crypto
Good Gaussian Sampling in Practice?

+ Leads to the most compact lattice signature schemes
+ Good asymptotic complexity
- Requires Floating-Point Arithmetic

FFO [D. Prest 2016]
Good Gaussian Sampling in Practice?

+ Leads to the most compact lattice signature schemes
+ Good asymptotic complexity
  
- Requires Floating-Point Arithmetic

FFO [D. Prest 2016]

Not so studied in practice so far . . .

**Wide impact:** signatures, homomorphic signatures, IBE, ABE, . . .
Solution 2: Fiat-Shamir transform

Idea: [Lyubashevski, . . ., BLISS, TESLA]

- Prove knowledge of a short vector without revealing it
- No need for a full basis
- Sampling potentially simpler
- Larger signatures.
Figure: A lattice and two puppies