Overview of Lattice based Cryptography

from Geometric Intuition to Basic Primitives

Léo Ducas

CWI, Amsterdam, The Netherlands

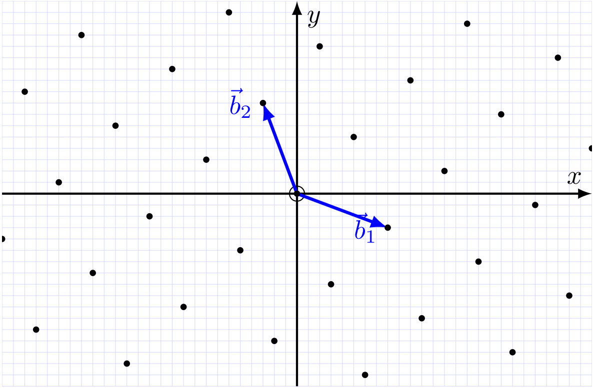
Spring School on Lattice-Based Cryptography
Oxford, March 2017

Content of the talk

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

Outline

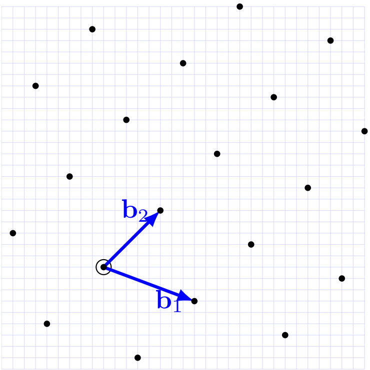
Lattices !



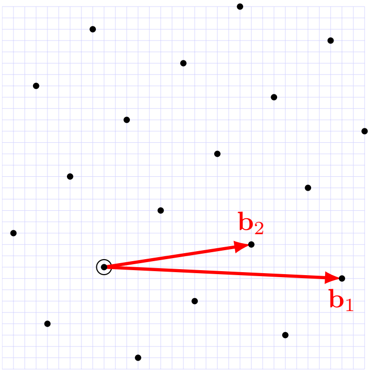
Definition

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

G $\rightarrow$ **B** : easy (randomization);

B $\rightarrow$ **G** : hard (LLL, BKZ, Lattice Sieve...).

An important invariant: the Volume

For any two bases $\mathbf{G}$, $\mathbf{B}$ of the same lattice Λ:

$$\det(\mathbf{G}\mathbf{G}^t) = \det(\mathbf{B}\mathbf{B}^t).$$

We can therefore define:

$$\mathrm{vol}(\Lambda) = \sqrt{\det(\mathbf{G}\mathbf{G}^t)}.$$

Geometrically: the volume of any **fundamental domain of** Λ.

An important invariant: the Volume

For any two bases $\mathbf{G}, \mathbf{B}$ of the same lattice Λ:

$$\det(\mathbf{G}\mathbf{G}^t) = \det(\mathbf{B}\mathbf{B}^t).$$

We can therefore define:

$$\mathrm{vol}(\Lambda) = \sqrt{\det(\mathbf{G}\mathbf{G}^t)}.$$

Geometrically: the volume of any **fundamental domain of** Λ.

Let $\mathbf{G}^\star$ be the Gram-Schmidt Orthogonalization of $\mathbf{G}$

$\mathbf{G}^\star$ is **not** a basis of Λ, nevertheless:

$$\mathrm{vol}(\Lambda) = \sqrt{\det(\mathbf{G}^\star \mathbf{G}^{\star t})} = \prod \|\mathbf{g}_i^\star\|.$$

What is a “Good” basis

Recall that, independently of the basis $\mathbf{G}$ it hold that:

$$\mathrm{vol}(\Lambda) = \prod \|\mathbf{g}_i^\star\|.$$

Therefore, it is somehow equivalent that

- $\max_i \|\mathbf{g}_i^\star\|$ is small
- $\min_i \|\mathbf{g}_i^\star\|$ is large
- $\kappa(\mathbf{G}) = \min_i \|\mathbf{g}_i^\star\| / \max_i \|\mathbf{g}_i^\star\|$ is small

What is a "Good" basis

Recall that, independently of the basis $\mathbf{G}$ it hold that:

$$\mathrm{vol}(\Lambda) = \prod \|\mathbf{g}_i^\star\|.$$

Therefore, it is somehow equivalent that

- $\max_i \|\mathbf{g}_i^\star\|$ is small
- $\min_i \|\mathbf{g}_i^\star\|$ is large
- $\kappa(\mathbf{G}) = \min_i \|\mathbf{g}_i^\star\| / \max_i \|\mathbf{g}_i^\star\|$ is small

Good basis (rule of thumb)

$$\kappa(\mathbf{G}) = \mathrm{poly}(d), \qquad \forall i, \|\mathbf{g}_i^\star\| = \mathrm{poly}(d) \cdot \mathrm{vol}(\Lambda)^{1/d}.$$

What is a "Good" basis

Recall that, independently of the basis $\mathbf{G}$ it hold that:

$$\mathrm{vol}(\Lambda) = \prod \|\mathbf{g}_i^\star\|.$$

Therefore, it is somehow equivalent that

- $\max_i \|\mathbf{g}_i^\star\|$ is small
- $\min_i \|\mathbf{g}_i^\star\|$ is large
- $\kappa(\mathbf{G}) = \min_i \|\mathbf{g}_i^\star\| / \max_i \|\mathbf{g}_i^\star\|$ is small

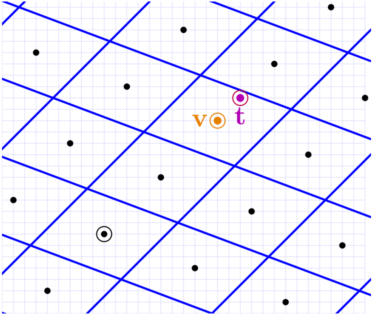
Good basis (rule of thumb)

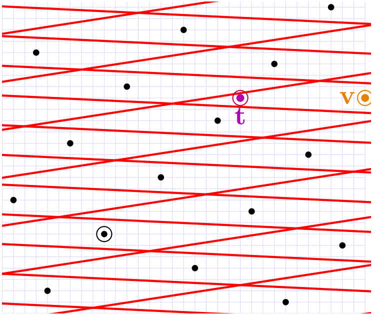
$$\kappa(\mathbf{G}) = \mathrm{poly}(d), \qquad \forall i, \|\mathbf{g}_i^\star\| = \mathrm{poly}(d) \cdot \mathrm{vol}(\Lambda)^{1/d}.$$

LLL-reduced basis (rule of thumb)

$$\kappa(\mathbf{G}) \approx (1.04)^d, \qquad \max_i \|\mathbf{g}_i^\star\| \approx (1.02)^d \cdot \mathrm{vol}(\Lambda)^{1/d}.$$

Each basis defines a **parallelepipedic tiling**.

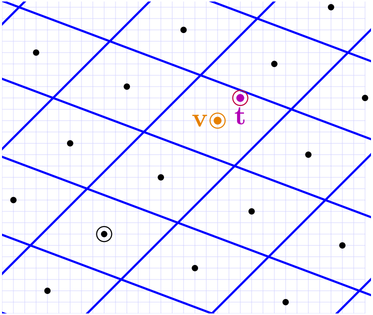


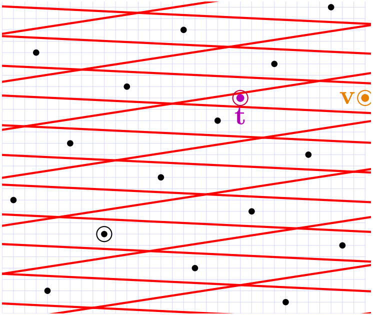


Round'off Algorithm [Lenstra, Babai]:

Bases and Fundamental Domains

Each basis defines a **parallelepipedic tiling**.

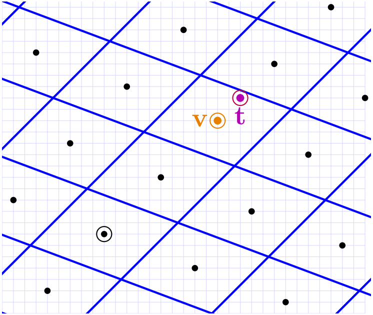


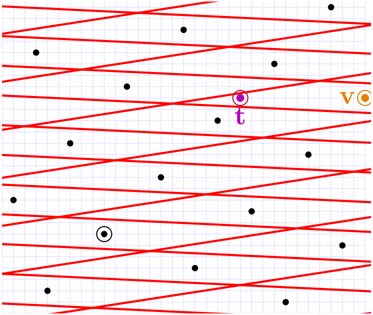


Round'off Algorithm [Lenstra, Babai]:

- Given a target **t**

Each basis defines a **parallelepipedic tiling**.

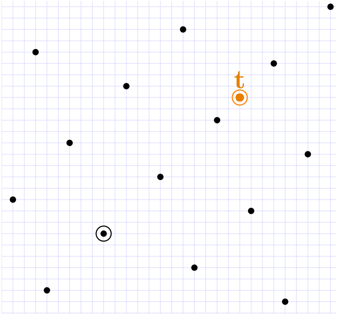




Round'off Algorithm [Lenstra, Babai]:

- Given a target **t**
- Find's **v** $\in L$ at the center the tile.

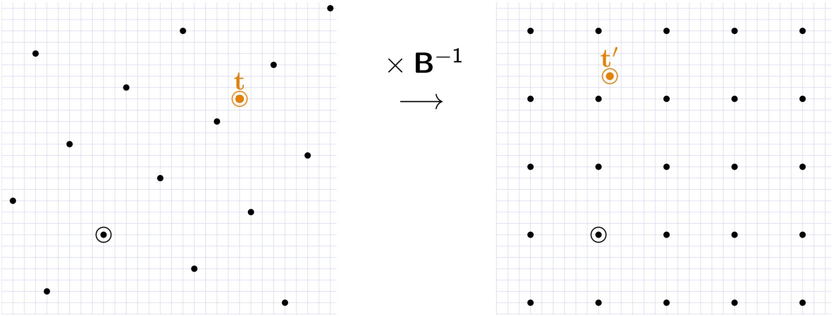
Round'off Algorithm



$\longrightarrow$

ROUNDOFF Algorithm [Lenstra,Babai]:

Round'off Algorithm

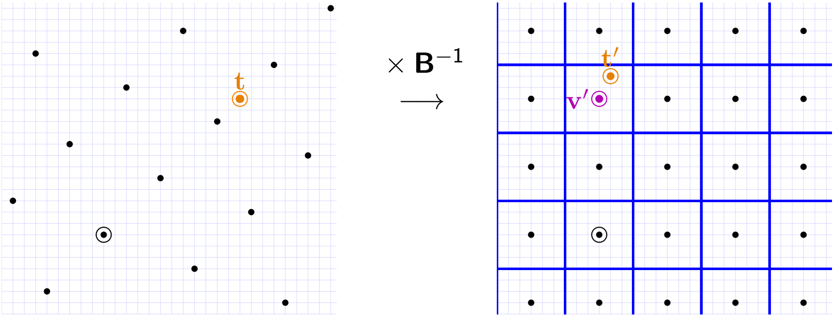


RoundOff Algorithm [Lenstra,Babai]:

- Use $\mathbf{B}$ to switch to the lattice $\mathbb{Z}^n$ ($\times \mathbf{B}^{-1}$)

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t};$$

Round'off Algorithm

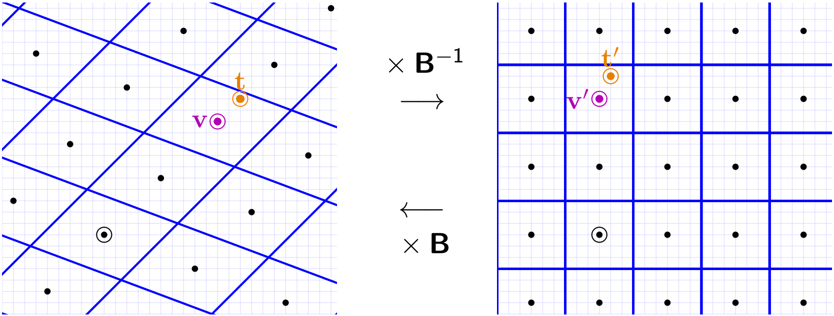


ROUNDOFF Algorithm [Lenstra,Babai]:

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

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil;$$

Round'off Algorithm



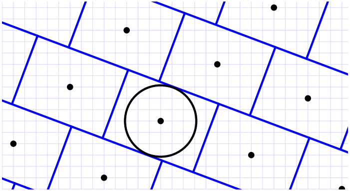
ROUNDOFF Algorithm [Lenstra,Babai]:

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

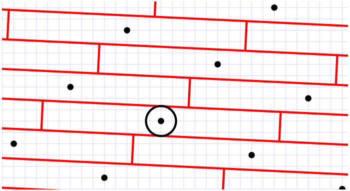
$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

Nearest-Plane Algorithm

There is a better algorithm (NearestPlane) based on Gram-Schmidt Orth. $\mathbf{B}^\star$ of a basis $\mathbf{B}$:



Decoding radius with $\mathbf{G}^\star$



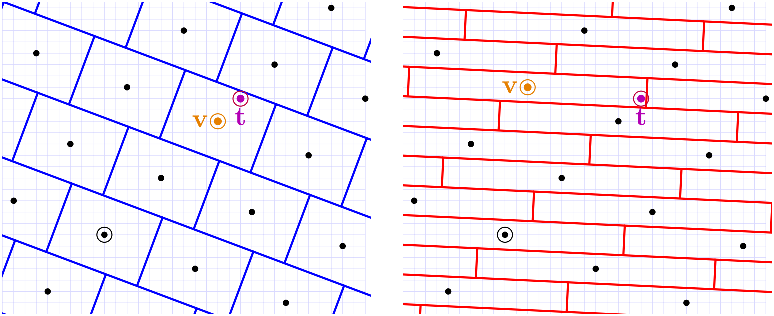
Decoding radius with $\mathbf{B}^\star$

- Worst-case distance: $\frac{1}{2}\sqrt{\sum \|\mathbf{b}_i^\star\|^2}$ (Approx-CVP)
- Correct decoding of $\mathbf{t} = \mathbf{v} + \mathbf{e}$ where $\mathbf{v} \in \Lambda$ if (BDD)

$$\|\mathbf{e}\| \leq \min \|\mathbf{b}_i^\star\|$$

Trapdoors from Lattices ?

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 ?

Encryption from lattices (simplified)

Using the (second) decoding algorithm, one can recover $\mathbf{v}, \mathbf{e}$ from $\mathbf{w} = \mathbf{v} + \mathbf{e}$ when

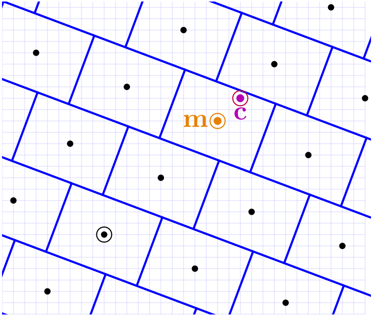
$$\|\mathbf{e}\| \leq \min \|\mathbf{b}_i^*\|$$

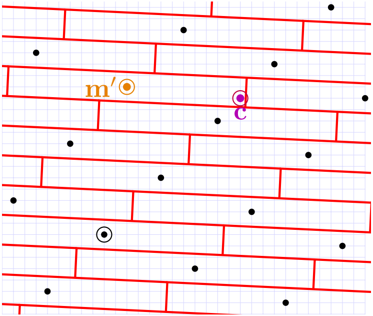
Fix a parameter η:

- Private key: good basis $\mathbf{G}$ such that $\|\mathbf{g}_i^*\| \geq \eta$
- Public key: bad basis $\mathbf{B}$ such that $\|\mathbf{b}_i^*\| \ll \eta$
- Message : $\mathbf{m} \in \Lambda = \mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{G})$
- Ciphertext : $\mathbf{c} = \mathbf{m} + \mathbf{e}$, for a random error $\mathbf{e}$, $\|\mathbf{e}\| \leq \eta$
- Decryption : $(\mathbf{m}', \mathbf{e}) = \textsc{NearestPlane}(\mathbf{c})$

Encryption from lattices

Decryption : $(\mathbf{m}', \mathbf{e}) = \mathit{decode}(\mathbf{c})$





- With the good basis **G**, $\mathbf{m}' = \mathbf{m}$
- With the bad basis **B**, $\mathbf{m}' \neq \mathbf{m}$: decryption fails !

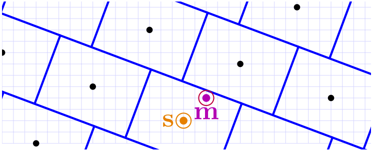
Signatures

Sign

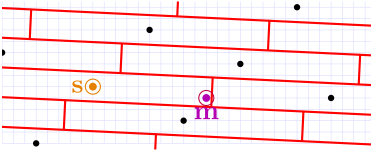
- Hash the message to a random vector $\mathbf{m}$.
- apply NearestPlane with a good basis $\mathbf{G}$:
  find $\mathbf{s} \in L$ close to $\mathbf{m}$.

Verify

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



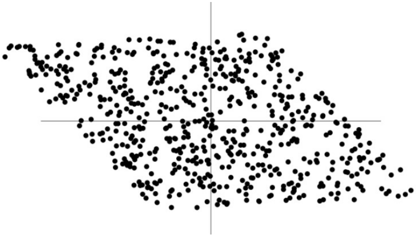
Correct signature (close)



Incorrect signature (far)

A statistical attack [NguReg06,DucNgu12]

The difference $\mathbf{s} - \mathbf{m}$ is always inside the parallelepiped spanned by the good basis $\mathbf{G}$ (or its GSO $\mathbf{G}^\star$):



Each signatures $(\mathbf{s}, \mathbf{m})$ leaks a bit of information about $\mathbf{G}$.
Learning a parallepiped from few signatures [Nguyen Regev 2006]:

$\Rightarrow$ Total break of original GGH and NTRUSign schemes.

Gaussian sampling

Randomize the previous algorithms (Gaussian-sampling):
the distribution $\mathbf{s} - \mathbf{m}$ can be made **independent** of $\mathbf{G}$

- [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

Construction of q-ary lattice (Primal / Construction A)

Let q be a prime[1] integer, and $n < m$ two positive integers.
The matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ spans the q-ary lattice:

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

Lattice parameters

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

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

[1] Not necessarly, but simpler.

Construction of q-ary lattice (Dual / Parity-Check)

Let q be a prime[2] integer, and $n < m$ two positive integers.
The matrix $\mathbf{A}^t \in \mathbb{Z}_q^{n \times m}$ is the parity-check of the lattice:

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

Lattice parameters

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

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

[2] Not necessarly, but simpler.

The Short Integer Solution Problem (SIS)

Definition (SIS assumption)

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

The Short Integer Solution Problem (SIS)

Definition (SIS assumption)

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

Lattice formulation

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

Worst-case to average case connection due to [Ajtai 1998].

Simple application of SIS

Set $\mathcal{S} = \{0,1\}^m$ and consider the function:

$$f_{\mathbf{A}} : \mathcal{S} \to \mathbb{Z}_q^n, \qquad \mathbf{x} \mapsto \mathbf{A}^t \mathbf{x} \bmod q$$

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

- Finding collision[3] is as hard as SIS (take the difference)

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

- $f_{\mathbf{A}}$ 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 χ be a distribution of small errors $\ll q$.

Definition (Decisional LWE)

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

Definition (Search LWE)

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

Both problems are easily proved equivalent.

The Learning With Error problem (LWE)

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

Definition (Decisional LWE)

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

Definition (Search LWE)

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

Both problems are easily proved equivalent.

Lattice formulation

Solving BDD in $\Lambda_q(\mathbf{A})$ is **hard**.

Worst-case to average case connection due to [Regev 2005].

LWE as unique-SVP (The embedding technique)

Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$, consider

$$\Lambda = \Lambda_q(\mathbf{A}, \mathbf{b})$$

Then:

- $\mathbf{e} \in \Lambda$, and $\|\mathbf{e}\| \approx \sigma\sqrt{m}$
- 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 $\Lambda_q(\mathbf{A}, \mathbf{b})$ is **hard**.

Simple application of LWE

Set $\mathcal{S} = \{-\sigma, \dots \sigma\}^m$ and consider the function:

$$g_{\mathbf{A}} : \mathbb{Z}_q^n \times \mathcal{S} \to \mathbb{Z}_q^m, \qquad (\mathbf{s}, \mathbf{e}) \mapsto \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$$

LWE $\Rightarrow$ Secret-Key Encryption

Idea : Noisy one-time pad

- $Enc_{\mathbf{s}}(m \in \{0,1\}) = (\mathbf{a}, \mathbf{a}^t\mathbf{s} + e + \lfloor \frac{q}{2} \rceil m)$
- $Dec_{\mathbf{s}}(\mathbf{a}, b) = \lfloor \frac{2}{q}(b - \mathbf{a}^t\mathbf{s}) \rceil \bmod 2$

Outline

Encryption is easy

Idea:

- Use one short lattice vector (rather than a full good basis $\mathbf{B}$)
- This short vector is easy to hide: LWE as unique-SVP

Public Key Encryption, [Regev 2005]

$m \gg n \log q$.

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

$$d = y - \mathbf{x}^t \mathbf{s} = \mathbf{t}^t \mathbf{e} + e + \lfloor \frac{q}{2} \rceil m$$

and return $m = \lfloor \frac{2}{q} d \rceil \bmod 2$

Public Key Encryption, [Regev 2005]

$m \gg n \log q$.

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

$$d = y - \mathbf{x}^t\mathbf{s} = \mathbf{t}^t\mathbf{e} + e + \lfloor \frac{q}{2} \rceil m$$

and return $m = \lfloor \frac{2}{q} d \rceil \bmod 2$

Proof sketch for CPA security

- Replace PK by uniform random $(\mathbf{A}, \mathbf{b})$
- Apply the left-over hash lemma on $\mathbf{t}$ over $(\mathbf{A}, \mathbf{b})$
- $Enc(m)$ is statistically close to uniform.

PKE / Approx. Key-Exchange [Lindner Peikert 2011]

Using a Systematic-Normal form, one can assume that $\mathbf{s} \leftarrow \chi^n$ is small as well. Take $m = n$.

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

$$d = y - \mathbf{x}^t\mathbf{s} = \mathbf{s}^t\mathbf{e}' + \mathbf{s}'^t\mathbf{e} + e + \lfloor \frac{q}{2} \rceil m$$

and return $m = \lfloor \frac{2}{q} d \rceil \bmod 2$

Using a Systematic-Normal form, one can assume that $\mathbf{s} \leftarrow \chi^n$ is small as well. Take $m = n$.

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

$$d = y - \mathbf{x}^t\mathbf{s} = \mathbf{s}^t\mathbf{e}' + \mathbf{s}'^t\mathbf{e} + e + \lfloor\frac{q}{2}\rceil m$$

and return $m = \lfloor\frac{2}{q}d\rfloor \bmod 2$

Proof sketch for CPA security

- Replace PK by uniform random by LWE assumptuion
- Replace $Enc(m)$ by uniform random by LWE assumptuion

Can also be made an approximate key Exchange.

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 ?

[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.

[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

Solution 1: Hash-Then-Sign

Sign

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

Verify

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

Ad-hoc construction of lattices with a good basis

Definition (The Matrix-NTRU assumption)

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

[5] $\mathbf{H}$ is provably uniform for midly large $\mathbf{F}, \mathbf{G}$ [Stehle Steinfeld 2012]
[6] IMHO: Precise parameter proposal not conservative enough

Ad-hoc construction of lattices with a good basis

Definition (The Matrix-NTRU assumption)

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

Do not overstreched !

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

[5] $\mathbf{H}$ is provably uniform for midly large $\mathbf{F}, \mathbf{G}$ [Stehle Steinfeld 2012]
[6] IMHO: Precise parameter proposal not conservative enough

Ad-hoc construction of lattices with a good basis

Definition (The Matrix-NTRU assumption)

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

Do not overstreched !

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

- $(\mathbf{F}, \mathbf{G})$ 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] $\mathbf{H}$ is provably uniform for midly large $\mathbf{F}, \mathbf{G}$ [Stehle Steinfeld 2012]
[6] IMHO: Precise parameter proposal not conservative enough

Provably secure construction of lattices with a good basis

SoA: [Micciancio Peikert 2012] "Simpler, Tighter, Faster, Smaller".

- Define a Gadget matrix $\mathbf{G} = [\mathbf{I}, 2\mathbf{I}, 4\mathbf{I}, \dots 2^k \mathbf{I}]$
- 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 $\Lambda^{\perp}(\mathbf{A})$

+ 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 FFO [D. Prest 2016]
- Requires Floating-Point Arithmetic

Good Gaussian Sampling in Practice ?

+ Leads to the most compact lattice signature schemes
+ Good asymptotic complexity FFO [D. Prest 2016]
- Requires Floating-Point Arithmetic

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.

Thanks !

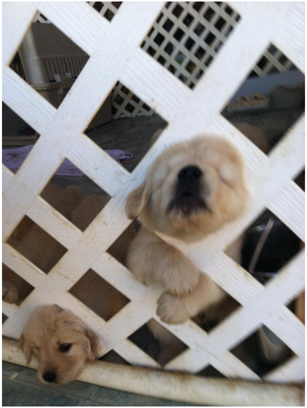


Figure: A lattice and two puppies