Advanced Cryptographic Primitives
Course 3: *The Learning With Errors Problem*

Teacher: Damien Stehlé
Scribe: Mihai-Ioan Popescu

22.09.2014

0 Introduction

The learning with errors problem (LWE):

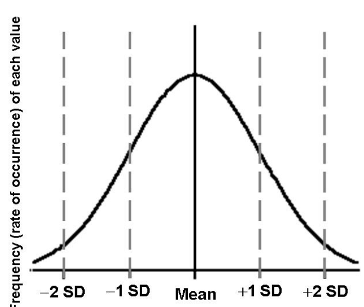
- Introduced by Oded Regev (2005) [8]
- Since then, very hot topic in cryptography $\implies$ Encryption, IBE, ABE (attribute-based encryption) for all circuits, FE (functional encryption), FHE (fully homomorphic encryption)
- Why is it insteresting to cryptographers?
  - ⋆ simple and reach problem (linear algebra $\rightsquigarrow$ easy to devise advanced primitives - which is the focus of this course)
  - ⋆ it leads to asymptotically efficient primitives
  - ⋆ very clean security grounding
  - ⋆ it seems to be quantum-resistant

1 Definition

1.1 Learning with errors (LWE)

References: Oded Regev survey [9], Laguillaumie, Langlois and Stehlé survey [5]

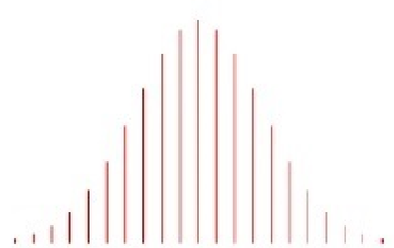
- Gaussian distribution: $D_{s,c}(x) \sim \exp(-\pi\frac{(x-c)^2}{s^2})$ **(proportionality)**
  s = standard deviation parameter (**SD**)
  c = center of the distribution (**Mean**)



Gaussian distribution (continuous)

- Integral Gaussian distribution: $D_{\mathbb{Z},s,c}(x) \sim \exp(-\pi\frac{(x-c)^2}{s^2})$

  $x \in \mathbb{Z}$ (whereas for the continous case, x is real)
  center c does not need to be an integer!



Integral Gaussian distribution

$D_{\mathbb{Z},s,c}(x) = \frac{\exp(-\pi(x-c)^2/s^2)}{\sum_{k\in\mathbb{Z}}\exp(-\pi(k-c)^2/s^2)}$

<u>*Note*:</u> Not all (nice) properties of the continuous case hold for the integral one! But may do, when s $\gg$ 1.

<u>2 properties we need today:</u>

1. We can sample from it in quasi-linear time (with respect to output size): see Ducas, Durmus, Lepoint, Lyubashevsky 2013 [3].

2. If $s \geq 1, \forall t > 0 : \Pr_{x \leftarrow D_{\mathbb{Z},s,c}}[|x-c| \geq t \cdot s] \leq 4 \cdot \exp(-\pi t^2)$ (see subsection 2.3 and 2.4 of Micciancio-Peikert 2012 [6])

LWE Distribution. Let $n \geq 1, q \geq 2, \alpha \in (0,1)$ and $\vec{s} \in (\mathbb{Z}_q)^n$. We define the distribution $D_{n,q,\alpha}(\vec{s})$ over $(\mathbb{Z}_q)^n \times \mathbb{Z}_q$ by:

| sample $a \leftarrow U(\mathbb{Z}_q^n)$, sample $e \leftarrow D_{\mathbb{Z},\alpha\cdot q,0}$ (the error term)
| return $(\vec{a}, <\vec{a}, \vec{s}> + e)$: the inner product of $\vec{a}$ with $\vec{s}$ + some noise e in $\mathbb{Z}$, then reduced mod q.

Search LWE. Let $\vec{s} \in \mathbb{Z}_q^n$ arbitrary. Given arbitrarily many samples from $D_{n,q,\alpha}(\vec{s})$, the goal is to find $\vec{s}$.

Decision LWE. Let $\vec{s} \leftarrow U(\mathbb{Z}_q^n)$. The goal is to distinguish between $D_{n,q,\alpha}(\vec{s})$ and $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, given arbitrarily many samples.

What does it mean to solve Decision-LWE ?

We have a PPT (probabilistic polynomial-time) algorithm $\mathcal{A}$ which makes sample requests and returns $b \in \{0,1\}$. It wins if with non-negligible probability over $\vec{s}$ (proportion $\geq \frac{1}{n^c}$, for some constant $c > 0$), we have:

$$Adv(\mathcal{A}) = \left| Pr[\mathcal{A} \overset{D(\vec{s})}{\to} 1] - Pr[\mathcal{A} \overset{U}{\to} 1] \right| \geq \frac{1}{n^{c'}}, \text{ for some } c' > 0$$

Matrix interpretation:

$$\underset{m\ rows}{} \overset{n\ cols}{\begin{pmatrix} \vdots \\ \mathbf{A} \\ \vdots \end{pmatrix}} \quad , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \mod \mathrm{q}$$

Each row is a fresh LHS (left-hand side) of $D_{n,q,\alpha}(\vec{s})$.

$m =$ the number of samples.

goal can be:

$\longrightarrow$ find $\vec{s}$.

$\longrightarrow$ tell that RHS (right-hand side) is not uniform (and independent from LHS).

***Remark*:** Why discrete Gaussians?

- Q: why discrete? continuous Gaussians works (replacing $\mathbb{Z}_q$ in RHS by $\mathbb{R}/q\mathbb{Z}$).
  A: simpler to explain with integers.
- Q: why Gaussian? E.g. rather than $U([\![-5\alpha q, +5\alpha q]\!])$?
  A: hardness proofs for LWE heavily rely on Gaussians.

***Remark*:**
$\longrightarrow$ If $\alpha = 0$, LWE is easy (no error, no noise): linear system mod q.
$\longrightarrow$ If $\alpha \approx 1$, LWE becomes trivially impossible as the samples contain almost no information on $\vec{s}$ (noise hides - covers - everything).

1.2 LWE search to decision reduction

Decision $\rightarrow$ search: easy!

- $\star$ ask samples
- $\star$ call Search-LWE oracle $\rightsquigarrow$ $\vec{s}$ or fail
- $\star$ if "fail" $\rightarrow$ reply "$U(\mathbb{Z}_q^n \times \mathbb{Z})$"
- $\star$ else if (RHS - $LHS \cdot \vec{s}$) is small $\rightarrow$ reply "LWE", else reply "Unif"

Theorem 1.1 *Assume that q is prime and $q \leq poly(n)$. Assume there exists a PPT algorithm $\mathcal{A}$ that has non-negligible distinguishing advantage between U and $D(\vec{s})$ with non-negligible probability over the choice of $\vec{s}$.*

Then there exists a PPT algorithm $\mathcal{B}$ that finds $\vec{s}$ from the samples from $D(\vec{s})$ with probability $\geq 1 - 2^{-n}$ for all $\vec{s}$ (over the internal randomness of $\mathcal{B}$ and randomness of $D(\vec{s})$ samples).

***Remark*:** The assumptions may be removed: see Brakerski, Langlois, Peikert, Regev, Sthelé 2013 [2].

Proof (3 steps)

step 1: Make the distinguishing advantage of $\mathcal{A} \geq 1 - 2^{-3n}$

Run $\mathcal{A} \rightarrow N$ times
If it returns 1 more than $N/2$ times then $\implies$ return 1, else 0.
* proof as exercise (*note that we have unlimmited access to samples!*)

step 2: Solve Search-LWE with non-negligible probability over $\vec{s} \leftarrow U(\mathbb{Z}_q^n)$

Consider an $\vec{s}$ such that the distinguishing advantage is $\geq 1 - 2^{-3n}$.
We are to recover $\vec{s_1}$, the 1^{st} coordinate of $\vec{s}$.
We try all s_1^* in $[0, q-1]$ and check whether $s_1 = s_1^*$ or not.

Given a sample $(\vec{a}, b)$ for $D(\vec{s})$, we construct a sample $(\vec{a}', b')$, where $\vec{a}'$ from $D(\vec{s})$ if $s_1 = s_1^*$ or else, from $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$:

$$u \leftarrow Unif(\mathbb{Z}_q) \text{ and } (\vec{a}, b) \longmapsto (\underbrace{\vec{a} + \begin{pmatrix} u \\ 0 \\ \vdots \\ 0 \end{pmatrix}}_{\text{uniform, thanks to } \vec{a}} , b + us_1^*).$$

$$b + us_1^* = < \vec{a} + \begin{pmatrix} u \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \vec{s} > -us_1 + us_1^* + e \ = < \vec{a} + \begin{pmatrix} u \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \vec{s} > +u(\underbrace{s_1^* - s_1}_{if 0 \implies +e}) + e$$

- If $s_1^* = s_1$, that is a sample from $D(\vec{s})$
- Else, $u(s_1^* - s_1)$ uniform (using q prime) $\implies$ RHS uniform, independent of LHS.

<u>step 3</u>: Solving Search-LWE for all $\vec{s}$ (using a solver that works for a non-negligible fraction of all $\vec{s}$'s):

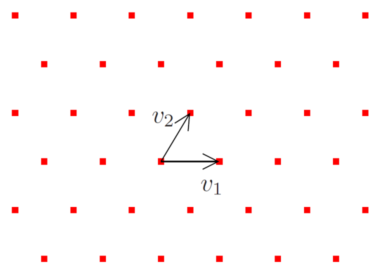
- let $(\vec{a}, \underbrace{b}_{<a,s>+e})$ from $D(\vec{s})$.
- Sample $\vec{t} \leftarrow U(\mathbb{Z}_q^n)$.
- Map $(\vec{a}, b)$ to $(\vec{a}, \underbrace{b + < \vec{a}, \vec{t} >}_{<\vec{a}, \vec{s} + \vec{t}> + e})$ $\implies$ it maps $D(\vec{s})$ to $D(\underbrace{\vec{s} + \vec{t}}_{uniform})$

With non-negligible probability, we can recover $\vec{s} + \vec{t}$ from samples from $D(\vec{s} + \vec{t})$. Then $\vec{s} = (\vec{s} + \vec{t}) - \vec{t}$.
<u>Note</u>: We will distinguish the $D(\vec{s} + \vec{t})$ distribution from U, for some $\vec{t}$, so pick as many $\vec{t}$'s as needed ■

2 Hardness of LWE

2.1 Euclidean lattices

Definition *(Lattice)*
A lattice is a set of the form $L = \sum_{i \leq n} \mathbb{Z}\vec{b_i}$ for linearly independent $\vec{b_i}$'s.
The $\vec{b_i}$'s - said basis, n - lattice dimension.



Lattice basis

Definition *(Minimum of L)*
The minimum of a lattice L (denoted by $\lambda(L)$) is the Euclidean norm of a shortest non-zero vector of the lattice:

$$\lambda(L) = \min_{\vec{b} \in L \setminus \{0\}} \|\vec{b}\|$$

Definition *(GapSVP)*
Let $n \geq 1, \gamma \geq 1$. Given a basis of a lattice L (dimension n) and $a \in \mathbb{R}, a > 0$, $GapSVP$ requires to reply:

| YES, if $\lambda(L) \leq a$
| NO, if $\lambda(L) \geq \gamma \cdot a$

(hardness increases with n, decreases with γ)

***Remark*: ** $GapSVP$ is

- NP-hard under randomized reductions, for $\gamma = 2^{(\log n)^{1-\varepsilon}}$, for all $\varepsilon > 0$ (Haviv-Regev 2007 [4]).
- In NP $\cap$ coNP for $\gamma = \sqrt{n}$ (Aharonov-Regev [1]) - hence, unlikely to be NP-hard.

- In P for $\gamma = 2^{n\frac{\log\log(n)}{\log(n)}}$ (Schnorr'87 [10] + Micciancio-Voulgaris'10 [7]).

  Best known algorithms:

  $\star$ for small $\gamma : 2^{O(n)}$ [7]

  $\star$ for $\gamma \geq poly(n) : (\frac{n}{\log\gamma})^{O(\frac{n}{\log\gamma})}$ [10]

Definition *(Bounded Distance Decoding Problem BDD_γ)*
Given L and $t \in \mathbb{R}^n$ such that there exists $\vec{b}$ with $\|\vec{t} - \vec{b}\| \leq \frac{\lambda(L)}{2\gamma}$, the goal is to find $\vec{b}$.

Best known algorithms: same as for $GapSVP$.

2.2 LWE as a lattice problem

$$L(A) \quad = \quad \left\{\vec{x} \in \mathbb{Z}^m \ : \ \exists \vec{s} \in \mathbb{Z}_q^n \ : \ \vec{x} = A \cdot \vec{s}\, [q]\right\} \quad = \quad \underbrace{A \cdot \mathbb{Z}_q^n + (q\mathbb{Z})^m}_{\text{see figure of } LWE \text{ matrix interpretation}}$$

<u>*Note*</u>: $dim(L(A)) = n$

- A $\cdot\vec{s} + \vec{e}$ is the $\vec{t}$ in BDD.
- A $\cdot\vec{s}$ is the $\vec{b}$ in $BDD \rightsquigarrow$ easy to recover $\vec{s}$ from A $\cdot\vec{s}$.

$\vec{b} - \vec{t} = \vec{e}$ and $\|\vec{e}\|$ is small $\implies$ Most efficient LWE solver relies on [10] and [7] for BDD_γ:

$$\left(\frac{n \cdot \log(q)}{\log^2(\alpha)}\right)^{O\left(\frac{n \cdot \log(q)}{\log^2(\alpha)}\right)} \approx 2^{\tilde{O}\left(\frac{n \cdot \log(q)}{\log^2(\alpha)}\right)}$$

<u>*Note*</u>: as α tends to 0, the exponent $O\left(\frac{n \cdot \log(q)}{\log^2(\alpha)}\right)$ tends to 0.

2.3 LWE at least as hard as lattice problems

Theorem 2.1 *(Regev'05 [8], Brakerski, Langlois, Peikert, Regev and Stehlé '13 [2])*

Let $\alpha, q > 0$ *such that* $\alpha q \geq 2\sqrt{n}$.

If q *prime and* $q \leq poly(n)$, *there exists a poly-time quantum reduction from* $GapSVP_{\gamma}^{(n)}$ *to* $LWE_{n,q,\alpha}$ *with* $\gamma = \widetilde{O}(n/\alpha)$. *For all* q, *there exists a poly-time classical reduction from* $GapSVP_{\gamma}^{\sqrt{n}}$ *to* $LWE_{n,q,\alpha}$, *with* $\widetilde{O}(n/\alpha) = \gamma$.

Note: soft-O notation ($\widetilde{O}$) is used to forget poly-logarithmic multiplicative terms.

Bibliography

[1] Dorit Aharonov and Oded Regev. Lattice problems in NP $\cap$ coNP. *J. ACM*, 52(5):749–765 (electronic), 2005.

[2] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *STOC'13*, pages 575–584, 2013.

[3] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. Cryptology ePrint Archive, 2013. `https://eprint.iacr.org/2013/383`.

[4] I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *Proc. of STOC*, pages 469–477. ACM, 2007.

[5] F. Laguillaumie, A. Langlois, and D. Stehlé. Chiffrement avancé à partir du problème learning with errors. Presses Universitaires de Perpignan, 2014. Chapitre de l'ouvrage "Informatique Mathématique, une photographie en 2014".

[6] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Proc. of Eurocrypt*, volume 7237 of *LNCS*, pages 700–718. Springer, 2012.

[7] D. Micciancio and P. Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proc. of SODA*. ACM, 2010.

[8] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of STOC*, pages 84–93. ACM, 2005.

[9] O. Regev. The learning with errors problem, 2010. Invited survey in CCC 2010, available at `http://www.cs.tau.ac.il/~odedr/`.

[10] C. P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theor. Comput. Science*, 53:201–224, 1987.