Introduction to LWE

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Cryptology 1 (2022/23)

Content

Why Learning with Errors (LWE)

- introduced by O. Regev (2005)
- no efficient quantum algorithm is known for LWE
- versatile – a basis for various schemes, e.g.
  - public-key encryption
  - identity-based encryption
  - fully homomorphic encryption
  - signature schemes (mostly based on RLWE)
- variant for better efficiency: RLWE (Ring LWE)
- can be reduced to worst-case hardness of some problems on lattices

LWE

- notation:
  - dimension $n \in \mathbb{Z}^+$ (primary security parameter)
  - integer q, usually $q = \mathrm{poly}(n)$ (sometimes q is a prime number)
  - secret vector $\mathbf{s} \in \mathbb{Z}_q^n$
  - matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, chosen uniformly random
  - error distribution χ on $\mathbb{Z}_q$
  - for odd q: $\mathbb{Z}_q = \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$, e.g. $\mathbb{Z}_{29} = \{-14, \ldots, 14\}$
  - error vector $\mathbf{e} = (e_1, \ldots, e_m) \in \mathbb{Z}_q^m$, where $e_i \leftarrow \chi$ (independent) for all i
  - $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$, where $\mathbf{s} \in \mathbb{Z}_q^n$, $\mathbf{b} \in \mathbb{Z}_q^m$
- linear equations with some "noise"
- sometimes an oracle formulation for LWE:
  - access to oracle $\mathcal{O}_s$ that produces $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$
  - $\mathbf{a} \in \mathbb{Z}_q^n$ (uniform random), $e \leftarrow \chi$, $b = \langle \mathbf{a}, \mathbf{s} \rangle + e$
  - above: m – number of samples

LWE – problems and observations

- Search LWE: find s for given $\mathbf{A}$, $\mathbf{b}$ (or access to $\mathcal{O}_s$)
- Decision LWE: distinguish access to $\mathcal{O}_s$ from access to an oracle that produces uniform random $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$
- assumption: Search/Decision LWE is hard (for suitable parameters)
- without noise ($\mathbf{e}$ is zero) – system of linear equations
  - can be solved easily (e.g. by Gaussian elimination)
- Gaussian elimination increases noise (up to the point where equations have no information on $\mathbf{s}$)
- too much noise (χ uniform on $\mathbb{Z}_q$)
  - any $\mathbf{s}$ is a plausible solution
  - identical distributions for Decision LWE

LWE – noise selection

- usually discrete Gaussian distribution
  - assumption in security proofs, reductions
  - for $\sigma, c \in \mathbb{R}$ define $\rho_{\sigma,c}(x) = \exp(-(x-c)^2/(2\sigma^2))$
  - (continuous) normal distribution (mean c, standard deviation σ):

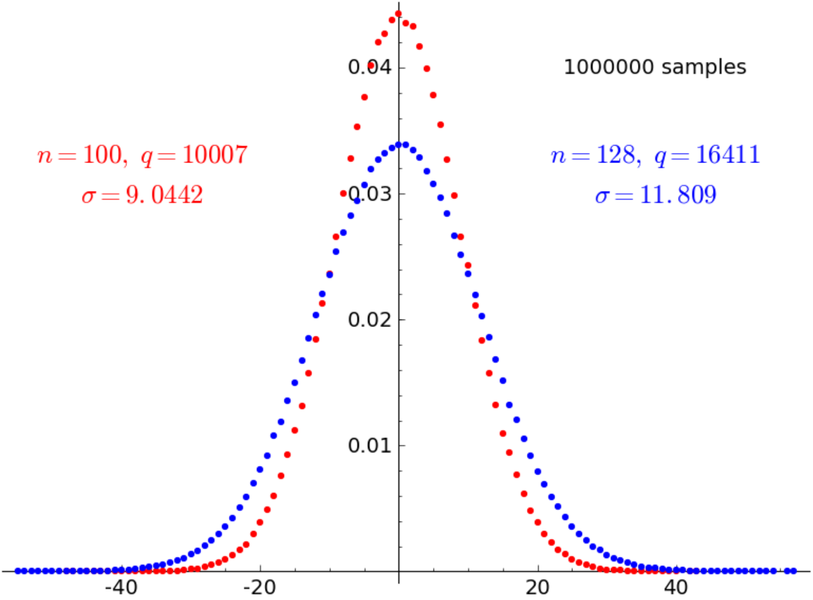
$$f_{\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\sigma\sqrt{2\pi}}$$

  - discrete Gaussian distribution $D_{\sigma,c}$ on $\mathbb{Z}$
    probability density function for $x \in \mathbb{Z}$:

$$f_{\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\sum_k \rho_{\sigma,c}(k)}$$

  - small noise for LWE: $c = 0$ and small σ
- other noise distributions studied
  - e.g. small uniform random (e.g. binary) errors for limited m (linear in n) (Micciancio, Peikert 2013)

Discrete Gaussian distr. – sampling in LWE instances



LWE – small example (1)

- $n = 5$, $q = 29$, $m = 8$,
- $\sigma = 0.95$

$$\underbrace{\begin{pmatrix} 11 & 19 & 3 & 14 & 0 \\ 13 & 22 & 19 & 17 & 27 \\ 15 & 9 & 18 & 19 & 28 \\ 19 & 19 & 12 & 12 & 28 \\ 24 & 26 & 9 & 28 & 3 \\ 18 & 6 & 25 & 28 & 0 \\ 23 & 18 & 21 & 17 & 11 \\ 13 & 16 & 19 & 4 & 21 \end{pmatrix}}_{\mathbf{A}} \cdot \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \end{pmatrix} \approx \underbrace{\begin{pmatrix} 6 \\ 19 \\ 28 \\ 14 \\ 8 \\ 9 \\ 5 \\ 20 \end{pmatrix}}_{\mathbf{b}} \pmod{29}$$

LWE – small example (2)

- solution:

$$\underbrace{\begin{pmatrix} 11 & 19 & 3 & 14 & 0 \\ 13 & 22 & 19 & 17 & 27 \\ 15 & 9 & 18 & 19 & 28 \\ 19 & 19 & 12 & 12 & 28 \\ 24 & 26 & 9 & 28 & 3 \\ 18 & 6 & 25 & 28 & 0 \\ 23 & 18 & 21 & 17 & 11 \\ 13 & 16 & 19 & 4 & 21 \end{pmatrix}}_{\mathbf{A}} \cdot \underbrace{\begin{pmatrix} 23 \\ 0 \\ 6 \\ 6 \\ 16 \end{pmatrix}}_{\mathbf{s}} + \underbrace{\begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ -2 \\ 2 \\ 0 \\ 1 \end{pmatrix}}_{\mathbf{e}} = \underbrace{\begin{pmatrix} 6 \\ 19 \\ 28 \\ 14 \\ 8 \\ 9 \\ 5 \\ 20 \end{pmatrix}}_{\mathbf{b}} \pmod{29}$$

Trivial algorithm for Search LWE

- maximum likelihood approach
- try all $\mathbf{s} \in \mathbb{Z}_q^n$ (i.e. q^n possibilities)
  - small error $\mathbf{e} = \mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ indicates a possible solution
  - the smallest error $\Rightarrow$ the most probable solution
  - l_2 norm computed in $\mathbb{R}$: $\|\mathbf{e}\| = \sqrt{e_1^2 + \ldots + e_n^2}$
- $O(n)$ equations for unique solution
- running time $O(q^n \cdot n^2)$
  - $\sim 2^{O(n \log n)}$ for typical q (polynomial in n)

Concrete bit security of LWE

n	q	σ	bit security
128	16411	11.809	**59**
256	65537	25.532	**120**
128	2053	2.705	**53**
256	4099	3.346	**109**
512	4099	2.900	**213**
1024	8209	3.528	**386**

Albrecht, Player and Scott: On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology 9(3):169–203. 2015

https://bitbucket.org/malb/lwe-estimator [estimated on 15 Nov 2016]

Decision LWE to Search LWE reduction

- trivial
- input: X – oracle access to $\mathcal{O}_s$ or uniform oracle for $(\mathbf{a}, b)$ pairs

  1. call Search LWE oracle, feeding it with pairs produced by X
  2. if Search LWE oracle returns $\mathbf{s}$ such that $e = b - \langle \mathbf{a}, \mathbf{s} \rangle$ is small for sufficiently many calls to X (producing $\mathbf{a}$ and b)
     then return "LWE"
  3. otherwise return "random"

Search LWE to Decision LWE reduction (idea)

- input: access to $\mathcal{O}_s$, and access to Decision LWE oracle
- main idea: guess and test the value of a coordinate
- testing if $s_1 = s_1' \in \mathbb{Z}_q$:
  1. let $(\mathbf{a}, b)$ be a sample from $\mathcal{O}_s$
     let $\mathbf{a}' = \mathbf{a} + (r, 0, \dots, 0)^T$ for $r \in \mathbb{Z}_q$
  2. we have $\langle \mathbf{a}', \mathbf{s} \rangle + e = b + rs_1$, for $r \in \mathbb{Z}_q$
  3. for uniform random r: $(\mathbf{a}', b + rs_1')$ is
     – LWE pair if $s_1 = s_1'$ (distributed accordingly, $\mathbf{a}'$ is uniform random)
     – uniform random if $s_1 \neq s_1'$ (difference $r(s_1 - s_1')$ is uniform$^{(*)}$)
     decide using Decision LWE oracle (iterating + Chernoff bound for negligible error)
- similarly for other coordinates
- running time: $O(nq)$ iterations (efficient for $q \leq \text{poly}(n)^{(**)}$)
- there is a reduction without assuming q being a prime number$^{(*)}$ and at most polynomial in $n^{(**)}$ (Brakerski et al. 2013)

Worst case to average case reduction (Search LWE)

- solving LWE for all $\mathbf{s}$ if we can solve it for non-negligible fraction of $\mathbb{Z}_q^n$
- input: $(\mathbf{A}, \mathbf{b})$
- iteration:
  1. choose uniform random $\mathbf{t} \in \mathbb{Z}_q^n$
  2. try solving LWE for $(\mathbf{A}, \mathbf{b} + \mathbf{A} \cdot \mathbf{t}) \mapsto \mathbf{s}'$
     if $\mathbf{s}$ is solution for LWE instance $(\mathbf{A}, \mathbf{b})$ then $\mathbf{s} + \mathbf{t}$ is a solution for the transformed instance:

     $$\mathbf{A} \cdot (\mathbf{s} + \mathbf{t}) = \mathbf{A} \cdot \mathbf{s} + \mathbf{A} \cdot \mathbf{t} = (\mathbf{b} + \mathbf{A} \cdot \mathbf{t}) - \mathbf{e}$$

  3. if successful, compute $\mathbf{s} = \mathbf{s}' - \mathbf{t}$
- use multiple iterations to reduce failure probability
- polynomial if success probability is non-negligible
- similar approach for Decision LWE

Encryption scheme

- Regev (2005)
- private key: $\mathbf{s} \in \mathbb{Z}_q^n$
- public key: LWE instance $(\mathbf{A}, \mathbf{b})$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$
  - possible parameters: q between n^2 and $2n^2$, $m = 1.1 \cdot n \lg q$
  - $\alpha = 1/(\sqrt{n} \cdot (\lg n)^2)$, $\sigma = \alpha q/\sqrt{2\pi}$
- bit encryption ($\mu \in \{0, 1\}$):
  1. choose uniform random $\mathbf{r} \in \{0, 1\}^m$
  2. ciphertext: $(\mathbf{r}^T\mathbf{A}, \langle \mathbf{b}, \mathbf{r} \rangle + \mu \cdot \lfloor q/2 \rfloor)$
- decryption (ciphertext $(\mathbf{a}, b)$):

$$\begin{aligned} b - \mathbf{a}\mathbf{s} &= \langle \mathbf{b}, \mathbf{r} \rangle + \mu \cdot \lfloor q/2 \rfloor - \mathbf{r}^T\mathbf{A}\mathbf{s} \\ &= \langle \mathbf{A}\mathbf{s} + \mathbf{e}, \mathbf{r} \rangle + \mu \cdot \lfloor q/2 \rfloor - \mathbf{r}^T\mathbf{A}\mathbf{s} \\ &= \mathbf{r}^T(\mathbf{A}\mathbf{s} + \mathbf{e}) + \mu \cdot \lfloor q/2 \rfloor - \mathbf{r}^T\mathbf{A}\mathbf{s} = \mathbf{r}^T\mathbf{e} + \mu \cdot \lfloor q/2 \rfloor \end{aligned}$$

if the result is close to 0 output $\mu = 0$ (close to $q/2$, output $\mu = 1$)

Correctness and security

- very simple encryption and decryption
- correctness:
  - we need $|\mathbf{r}^T\mathbf{e}| < q/4$
  - choose parameters q, σ such that above condition is not satisfied with negligible probability
- IND-CPA secure
- not IND-CCA secure

PQC, FrodoKEM

- FrodoKEM: standard LWE (round 3 “alternate” algorithm for encryption/KEM)
  - not a finalist
  - computation in ring mod $q = 2^{15}$ for 128-bit security level, and $q = 2^{16}$ for 192 and 256-bit security levels
  - public-key matrix generated pseudorandomly from a public-key seed, …
  - sizes of various parameters (in bytes):

level	private key	public key	ciphertext	
128	19 888	9 616	9 720	*FrodoKEM-640*
192	31 296	15 632	15 744	*FrodoKEM-976*
256	43 088	21 520	21 632	*FrodoKEM-1344*

- more size-efficient schemes – algebraic lattices (structured), e.g. Ring-LWE, Module-LWE

Remarks on FrodoKEM

- NIST Status Report on the 2nd Round:

  Plain LWE itself is among the most studied and analyzed cryptographic problems in existence today. The resulting potential security advantages of FrodoKEM are paid for with far worse performance in all metrics than other lattice schemes. …

  Use of FrodoKEM would have a noticeable performance impact on high traffic TLS servers …

  FrodoKEM may be suitable for use cases where the high confidence in the security of unstructured lattice-based schemes is much more important than performance.
- single selected algorithm for encryption/KEM: Crystals-Kyber
  - learning-with-errors (LWE) problem over module lattices