Foundations of Lattice Cryptography

Lukas Helminger

Mathematical Foundations of Cryptography – WT 2019/20

Outline

Foundations of Lattice Cryptography

- Shortest Integer Solution (SIS)
- Learning with Errors (LWE)
- Regev's LWE Cryptosystem
- Ring-SIS
- Ring-LWE

Literature

The slides are based on the following sources

- **A Decade of Lattice Cryptography**, Chris Peikert

Foundations of Lattice Cryptography

Short Integer Solution (SIS)

Definition (SIS)

Given m uniformly random vectors $a_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $A \in \mathbb{Z}_q^{n \times m}$, find a nonzero integer vector $z \in \mathbb{Z}^m$ of norm $\|z\| \leq \beta$ such that

$$Az = 0 \in \mathbb{Z}_q^n.$$

Short Integer Solution (SIS)

Definition (SIS)

Given m uniformly random vectors $a_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $A \in \mathbb{Z}_q^{n \times m}$, find a nonzero integer vector $z \in \mathbb{Z}^m$ of norm $\|z\| \leq \beta$ such that

$$Az = 0 \in \mathbb{Z}_q^n.$$

- Without constraint on $\|z\|$, it is easy to find solution via Gaussian elimination.

Short Integer Solution (SIS)

Definition (SIS)

Given m uniformly random vectors $a_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $A \in \mathbb{Z}_q^{n\times m}$, find a nonzero integer vector $z \in \mathbb{Z}^m$ of norm $\|z\| \leq \beta$ such that

$$Az = 0 \in \mathbb{Z}_q^n.$$

- Without constraint on $\|z\|$, it is easy to find solution via Gaussian elimination.
- Corresponds to SVP in the following lattice

$$L(A) := \{z \in \mathbb{Z}^m : Az = 0 \in \mathbb{Z}_q^n\} \supset q\mathbb{Z}^m.$$

Learning with Errors (LWE)

Definition (LWE Distribution)

For a vector $s \in \mathbb{Z}_q^n$ called the secret, the LWE distribution $A_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing $a \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \leftarrow \chi$, and outputting

$$(a, b = s \cdot a + e \mod q).$$

Learning with Errors (LWE)

Definition (LWE Distribution)

For a vector $s \in \mathbb{Z}_q^n$ called the secret, the LWE distribution $A_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing $a \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \leftarrow \chi$, and outputting

$$(a, b = s \cdot a + e \mod q).$$

Definition (Search-LWE$_{n,q,\chi,m}$)

Given m independent samples $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ drawn from $A_{s,\chi}$ for a uniformly random $s \in \mathbb{Z}_q^n$ (fixed for all samples), find s.

Regev's LWE Cryptosystem

Gen: secret key is a random LWE secret $s \in \mathbb{Z}_q^n$; public key is some $m \approx (n+1)\log q$ samples $(a_i, b_i = s \cdot a_i + e_i) \in \mathbb{Z}_q^{n+1}$ drawn from $A_{s,\chi}$. Set

$$M = \begin{pmatrix} A \\ b^t \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}.$$

Regev's LWE Cryptosystem

Gen: secret key is a random LWE secret $s \in \mathbb{Z}_q^n$; public key is some $m \approx (n+1)\log q$ samples $(a_i, b_i = s \cdot a_i + e_i) \in \mathbb{Z}_q^{n+1}$ drawn from $A_{s,\chi}$. Set

$$M = \begin{pmatrix} A \\ b^t \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}.$$

Enc: $m \in \{0,1\}$, choose $x \leftarrow_{\$} \{0,1\}^m$, then

$$c \leftarrow Mx + \left(0, m\left\lfloor \frac{q}{2} \right\rceil\right) \in \mathbb{Z}_q^{n+1}.$$

Regev's LWE Cryptosystem

Gen: secret key is a random LWE secret $s \in \mathbb{Z}_q^n$; public key is some $m \approx (n+1)\log q$ samples $(a_i, b_i = s \cdot a_i + e_i) \in \mathbb{Z}_q^{n+1}$ drawn from $A_{s,\chi}$. Set

$$M = \begin{pmatrix} A \\ b^t \end{pmatrix} \in \mathbb{Z}_q^{(n+1)\times m}.$$

Enc: $m \in \{0,1\}$, choose $x \leftarrow_\$ \{0,1\}^m$, then

$$c \leftarrow Mx + \left(0, m\left\lfloor \frac{q}{2} \right\rceil\right) \in \mathbb{Z}_q^{n+1}.$$

Dec:

$$\begin{aligned}(-s,1)^t \cdot c = (-s,1)^t Mx + m\left\lfloor \frac{q}{2} \right\rceil = e^t x + m\left\lfloor \frac{q}{2} \right\rceil \\ \approx m\left\lfloor \frac{q}{2} \right\rceil\end{aligned}$$

LWE and Lattices

Definition (Bounded Distance Decoding Problem (BDD_γ))

Given a basis B of an n-dimensional lattice L and a target point $t \in \mathbb{R}^n$ with the guarantee that $\mathrm{dist}(t, L) < d = \lambda_1(L)/2\gamma(n)$, find the unique lattice vector $v \in L$ such that $\|t - v\| < d$.

LWE and Lattices

Definition (Bounded Distance Decoding Problem (BDD$_\gamma$))

Given a basis B of an n-dimensional lattice L and a target point $t \in \mathbb{R}^n$ with the guarantee that $\mathrm{dist}(t, L) < d = \lambda_1(L)/2\gamma(n)$, find the unique lattice vector $v \in L$ such that $\|t - v\| < d$.

Search-LWE can be seen as BDD problem in the lattice

$$L(A) := \{x \in \mathbb{Z}^m : \exists s \in \mathbb{Z}^n, x = As \mod q\} = A\mathbb{Z}_q^n + q\mathbb{Z}^m,$$

with target point $t = b$ and $\mathrm{dist}(b, L) = \|s\| \approx \sqrt{m} \cdot \sqrt{\mathrm{Var}(A_{s,\chi})}$.

Harndess of LWE

Definition (Decisional Approximate SVP (GapSVP$_\gamma$))

Given a basis B of an n-dimensional lattice L where either $\lambda_1(L) \leq 1$ or $\lambda_1(L) > \gamma(n)$, determine which is the case.

Harndess of LWE

Definition (Decisional Approximate SVP (GapSVP$_\gamma$))

Given a basis B of an n-dimensional lattice L where either $\lambda_1(L) \leq 1$ or $\lambda_1(L) > \gamma(n)$, determine which is the case.

Reduction from search LWE to GapSVP on arbitrary n-dimension lattices.

Ring-SIS

$R = \mathbb{Z}[X]/(X^n - 1)$, i.e. elements of R can be represented by integer polynomials of degree less than n.

Ring-SIS

$R = \mathbb{Z}[X]/(X^n - 1)$, i.e. elements of R can be represented by integer polynomials of degree less than n.

$R_q := R/qR = \mathbb{Z}_q[X]/(X^n - 1)$

Ring-SIS

$R = \mathbb{Z}[X]/(X^n - 1)$, i.e. elements of R can be represented by integer polynomials of degree less than n.

$R_q := R/qR = \mathbb{Z}_q[X]/(X^n - 1)$

Definition (Ring-SIS)

Given m uniformly random elements $a_i \in R_q$, defining a vector $\mathbf{a} \in R_q^m$, find $O \neq \mathbf{z} \in R^m$ of norm $\|z\| \leq \beta$ s.t.

$$\mathbf{a}^{\mathbf{T}} \cdot \mathbf{z} = \mathbf{0} \in R_q.$$

R-SIS versus SIS

In R-SIS each random element $a \in R_q$ corresponds to n related vectors in $a_i \in \mathbb{Z}_q^n$ in SIS:

R-SIS versus SIS

In R-SIS each random element $a \in R_q$ corresponds to n related vectors in $a_i \in \mathbb{Z}_q^n$ in SIS:

$$X^i \in R \longleftrightarrow e_{i+1} \in \mathbb{Z}^n$$

$$X^3 + 2X + 1 \in \mathbb{Z}[X]/(X^4 - 1) \longleftrightarrow (1, 0, 2, 1) \in \mathbb{Z}^4$$

R-SIS versus SIS

In R-SIS each random element $a \in R_q$ corresponds to n related vectors in $a_i \in \mathbb{Z}_q^n$ in SIS:

$$X^i \in R \longleftrightarrow e_{i+1} \in \mathbb{Z}^n$$

$$X^3 + 2X + 1 \in \mathbb{Z}[X]/(X^4 - 1) \longleftrightarrow (1, 0, 2, 1) \in \mathbb{Z}^4$$

Multiplication by $a \in R_q$ is a $\mathbb{Z}$-linear function from R to R_q

$$\Rightarrow \text{circular matrix } A_a \in \mathbb{Z}_q^{n \times n}.$$

R-SIS versus SIS

In R-SIS each random element $a \in R_q$ corresponds to n related vectors in $a_i \in \mathbb{Z}_q^n$ in SIS:

$$X^i \in R \longleftrightarrow e_{i+1} \in \mathbb{Z}^n$$

$$X^3 + 2X + 1 \in \mathbb{Z}[X]/(X^4 - 1) \longleftrightarrow (1, 0, 2, 1) \in \mathbb{Z}^4$$

Multiplication by $a \in R_q$ is a $\mathbb{Z}$-linear function from R to R_q

$$\Rightarrow \text{circular matrix } A_a \in \mathbb{Z}_q^{n \times n}.$$

This yields the correspondence between a R-SIS instance $\mathbf{a} = (a_1, \ldots, a_m) \in R_q^m$ and the (structured) SIS instance

$$A = \left[A_{a_1} \mid \cdots \mid A_{a_m}\right] \in \mathbb{Z}_q^{n \times nm}.$$

Geometry of Rings and Ideal lattices

What is a short vector in R?

- Coefficient embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{Z}^n$ depends on the choice of representatives of R.
- Canonical embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{R}$ independent of representatives of R.

Geometry of Rings and Ideal lattices

What is a short vector in R?

- Coefficient embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{Z}^n$ depends on the choice of representatives of R.
- Canonical embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{R}$ independent of representatives of R.

An ideal lattice is a lattice corresponding to an ideal in R under some embedding.

Geometry of Rings and Ideal lattices

What is a short vector in R?

- Coefficient embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{Z}^n$ depends on the choice of representatives of R.
- Canonical embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{R}$ independent of representatives of R.

An ideal lattice is a lattice corresponding to an ideal in R under some embedding. Ideals of R are closed under multiplication by X. Corresponds to rotation by one

coordinate in the coefficient embedding, i.e.

$$(x_1, \ldots, x_n) \in L \Rightarrow (x_{1+k}, \ldots, x_{n+k}) \in L.$$

Hardness and Efficiency of R-SIS (compared to SIS)

Hardness:

- Reduction to worst-case problems on ideal lattices.
- SVP appears to be very hard on ideal lattices.

Hardness and Efficiency of R-SIS (compared to SIS)

Hardness:

- Reduction to worst-case problems on ideal lattices.
- SVP appears to be very hard on ideal lattices.

Efficiency:

- Key size of order n instead of n^2.
- In addition, multiplication can be performed in quasi-linear time using FFT-like techniques.

Ring LWE

Definition (Ring-LWE distribution)

For an $s \in R_q$ called the secret, the ring-LWE distribution $A_{s,\chi}$ over $R_q \times R_q$ is sampled by choosing $a \in R_q$ uniformly at random, choosing $e \leftarrow \chi$, and outputting

$$(a, b = s \cdot a + e \mod q).$$

Ring LWE

Definition (Ring-LWE distribution)

For an $s \in R_q$ called the secret, the ring-LWE distribution $A_{s,\chi}$ over $R_q \times R_q$ is sampled by choosing $a \in R_q$ uniformly at random, choosing $e \leftarrow \chi$, and outputting

$$(a, b = s \cdot a + e \mod q).$$

Connection to LWE:
Given a R-LWE sample $(a, b = s \cdot a + e) \in R_q \times R_q$, we can transform it to n LWE samples

$$\left(A_a, b^t = s^t A_a + e^t\right) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n,$$

where A_a correspondence to multiplication by a.