TU Graz

SCIENCE
PASSION
TECHNOLOGY

Modern Public Key Cryptography

Lattice Cryptography

Lukas Helminger

May 26, 2021

Outline

Literature

The slides are based on the following sources

- **An Introduction to Mathematical Cryptography**, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
- **A Decade of Lattice Cryptography**, Chris Peikert
- **Talk: The Short Integer Solutions Problem and Cryptographic Applications** by Daniele Micciancio (Lattice Workshop Berkeley)

Hardness Proof of SIS

Recall

- SIS problem: Finding a short element in the kernel of Ajtai's function $f_A(z) := Az$.
- Solution exists if $\beta^2, m \geq n \log q$.
- SIS problem $\equiv$ SVP$_\gamma$.
- Solving average-case SIS problem is at least as hard as solving worst-case SIVP$_\gamma$.
- Ajtai's function is collision resistant.
- SIS admits minicrypt primitives (usable, but inefficient)

Short Integer Solution (SIS)

Definition (SIS, Ajtai's function)

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

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

$f_A(z) := Az \mod q$ is called Ajtai's function, i.e., we are interested in short vectors of the kernel of f_A.

We can look at the SIS problem as a short vector problem on so-called q-ary m-dimensional lattices.

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

Solving the SIS problems can be accomplished by finding a sufficiently short nonzero vector in $\mathcal{L}^{\perp}(A)$, where A is chosen uniformly at random.

Hardness of SIS

Theorem

For any $m = \mathrm{poly}(n)$, any $\beta > 0$, and any sufficiently large $q \geq \beta \cdot \mathrm{poly}(n)$, solving $\mathsf{SIS}_{n,q,\beta,m}$ with non-negligible probability is at least as hard as solving SIVP_γ on arbitrary n-dimensional lattices with overwhelming probability, for some $\gamma = \beta \cdot \mathrm{poly}(n)$.

Proof.

Whiteboard. □

Ring-SIS

Preleminaries

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

$$R = \mathbb{Z}[X]/(X^4 - 1), \text{ every } f(X) \in R \text{ can be written as}$$
$$f(X) = \alpha_3 X^3 + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \text{ with } \alpha_i \in \mathbb{Z}.$$

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

$$R_{11} = \mathbb{Z}_{11}[X]/(X^4 - 1), \text{ every } f(X) \in R_{11} \text{ can be written as}$$
$$f(X) = \alpha_3 X^3 + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \text{ with } \alpha_i \in \mathbb{Z}_{11}.$$

- Endow R with a norm $\| \cdot \|$ (more details later).

Ring-SIS

Definition (Ring-SIS)

Given m uniformly random elements $a_i \in R_q$, defining a vector $\mathbf{a} \in R_q^m$, find $0 \neq \mathbf{z} \in R^m$ of norm $\|\mathbf{z}\| \leq \beta$ s.t.

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

Efficiency:

- Guarantee of existence of solution: $m \approx \log q$
  What does this imply for our last example? (Key size, Runtime)
- Using FFT-like techniques one can compute $a_i \cdot z_i$ in quasi-linear time.

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

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. (useful for developing intuition)
- Canonical embedding: $\sigma : \mathbb{Z}[X] \to \mathbb{C}^n$ independent of representatives of R. (used in security proofs)

Let $f(X) := X^3 + 2X + 1 \in \mathbb{Z}[X]/(X^4 - 1)$, then

$$\|f(X)\| := \left\| \begin{matrix} 1 \\ 0 \\ 2 \\ 1 \end{matrix} \right\| = \sqrt{6}.$$

Ideal Lattices

Let R be a ring. A subring $I \subset R$ is called an ideal in R if

$$\forall r \in R \forall a \in I : ar \in I.$$

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.,

$$(1, 2, 3, 4) \in L \Rightarrow (4, 1, 2, 3) \in L.$$

Hardness of R-SIS

Known hardness proofs for R-SIS relate to problems on ideal lattices.

Hardness:

- SVP and SIVP problems are equivalent: Symmetries in ideal lattices allow us to convert one short vector in n lin. ind. vectors of the same length.
- Again reduction to worst-case problems
- SVP appears to be very hard on ideal lattices, but ideal lattices have not been investigated as much as arbitrary lattices from a computational view.

Collision Resistance

It depends on the ring R...

- If $R = \mathbb{Z}[X]/(X^n - 1)$ is not collision resistant $\Rightarrow$ homogeneous R-SIS is easy. (R is not an integral domain)
- If $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n, then $f_{\mathbf{a}}$ is collision resistant, assuming that SVP_γ is hard for ideal lattices in R.

Summary

- Instead of integers the elements in R-SIS are integer polynomials (mod q) of degree n.
- Existence of solution: m doesn't depend on n ($m \approx \log q$)
  $\rightsquigarrow$ better efficiency (Key size of order n instead of n^2)
- R-SIS instance yields several structured SIS instances.
- R-SIS reduces to SVP_γ on ideal lattices.

Learning with Errors (LWE)

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

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

LWE Problems

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.

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

Given m independent samples $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where every sample is distributed according to either:

(i) $A_{s,\chi}$ for a uniformly random $s \in \mathbb{Z}_q^n$ (fixed for all samples), or

(ii) the uniform distribution,

distinguish which is the case.

LWE and Lattices

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

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

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

Hardness of LWE

Theorem ([Reg05])

For any $m = \mathrm{poly}(n)$, any modulus $q \leq 2^{\mathrm{poly}(n)}$, and any (discretized) Gaussian distribution χ of parameter $\alpha q \geq 2\sqrt{n}$ where $0 < \alpha < 1$, solving the decision-LWE$_{n,q,\chi,m}$ problem is at least as hard as quantumly solving SIVP$_\gamma$ on arbitrary n-dimensional lattices, for some $\gamma = O(n/\alpha)$.

Proof.

Whiteboard. For a classical reduction see [Pei09]. $\square$

Decision-LWE reduces to SIVP$_\gamma$ on arbitrary n-dimension lattices.

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.

What you should know...

- Proof sketch of SIS hardness
- Ring-SIS (relation to SIS, efficiency, hardness)
- LWE (definition, hardness)

Further Reading I

[Pei09] Chris Peikert.
Public-key cryptosystems from the worst-case shortest vector problem: extended abstract.
In *STOC*, pages 333–342. ACM, 2009.

[Reg05] Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In *STOC*, pages 84–93. ACM, 2005.