Part II Average-Case Lattice Problems

4. Short Integer Solution (SIS)

1996, Ajtai

4.1. Definitions

Def 19. (SIS)

$n, m, q > 0 \in \mathbb{N}$

$\beta > 0 \in \mathbb{R}$

Given $A \in \mathbb{Z}_q^{n \times m} = [\vec{a}_1, \vec{a}_2, \cdots \vec{a}_m]$

($\vec{a}_j$ are all sampled uniformly at random over $\mathbb{Z}_q^n$)

the problem $SIS_{n,m,q,\beta}$ asks to find a non-zero vec $\vec{z} \in \mathbb{Z}^m$ of norm $\|\vec{z}\| \leq \beta$ st.

$$A\vec{z} = \sum_i z_i \vec{a}_i = \vec{0} \mod q$$

choice of params

if fix m, n, q. smaller β → harder prob

but β & m should be large enough → sol exists

$$m \geq \log_2(q^n)$$
$$\beta \geq \sqrt{m}$$

⇒ if a vec $\vec{x} \in \{0,1\}^m$, the possible vec space is $2^m \geq q^n$.

$\Rightarrow \exists\ \vec{x} \neq \vec{x}' \in \{0,1\}^m$ s.t. $A\vec{x} = A\vec{x}'$

the coefficients of $A\vec{x} \in [0, q)$

$A\vec{x} \in \mathbb{Z}_q^n \Rightarrow q^n$ possible outcomes

$2^m \geq q^n \Rightarrow$ ←

$\Rightarrow \vec{z} = \vec{x} - \vec{x}' \in \{-1, 0, 1\}^m$ is a sol of $\|\vec{z}\| \leq \beta$

$\|\vec{z}\| = \sqrt{|z_1|^2 + \cdots + |z_m^2|}$

$\leq \sqrt{m} \leq \beta$.

- SIS is a surjective problem.
- SIS easier when larger m

  harder when larger n

	larger
easier	m, β
harder	n

SIS params vs. hardness.

(when fixed other params)

Hidden Lattice Problem.

- SIS → a problem over random q-ary lattices

★ SIS defines an instance of SVP$_\gamma$ in the random lattice

$$\Lambda_q^{\perp}(A) = \{\vec{y} \in \mathbb{Z}^m : A\vec{y} = \vec{0} \bmod q\}$$

i.e.

Base $A \in \mathbb{Z}_q^{n \times m}$. n-dim Λ

q-ary lattice $\Lambda_q^{\perp}(A)$ as before

SVP_γ SIS: find $\vec{z} \neq \vec{0}$ st. $\|\vec{z}\| \leq \gamma \cdot \lambda_1(\Lambda_q^{\perp}(A))$

$\gamma \cdot \lambda_1(\Lambda_q^{\perp}(A))$ depends on β.

i.e. $\gamma(n, \beta)$

Inhomogenous version (ISIS)

$\vec{t} \in \mathbb{Z}_q^n$ replace $\vec{0}$

i.e. $A\vec{z} = \vec{t} \mod q$

- Thus, SIS is a special case of ISIS.
- But, SIS is easier to work with from a lattice perspective.
- Another prob: Knapsack prob

  sampling some $\vec{z}$. compute $\vec{t} = A\vec{z} \mod q$

  - recover $\vec{z}$
  - distinguish $\vec{t}$ from a random var.

  it's injective, rather than surjective

Hermite Normal Form (HNF)

(can review Micciancio's LBC course notes

Vadim's Basic Lattice Cryptography

to better understand this)

$A \in \mathbb{Z}_q^{n \times m} = [A_1 \mid A_2]$

$A_1 \in \mathbb{Z}_q^{n \times n}$

$A_2 \in \mathbb{Z}_q^{n \times (m-n)}$

$A^{-1} \cdot A = [I_n \mid A^{-1} A_2]$

$\Rightarrow$ can work with $\Lambda_q^{\perp}([I_n \mid A^{-1}A_2])$

(good for practical use. will later explain in other notes)

4.2 Hardness

- lots of works show:

SIS (under specific parameter choices) is at least as hard (ALAHA) as solving $\begin{cases} SIVP_\gamma \\ GapSVP_\gamma \end{cases}$ on any lattice

→ worse-case to avg case

Thm 20

For any $m = poly(n)$

any $\beta > 0$

any $q \geq \beta \cdot poly(n)$

solving $SIS_{n,q,\beta,m}$ with non-negligible probability is ALAHA solving the problem $GapSVP_\gamma$ & $SIVP_\gamma$ on $\forall$ n-dim lattices with non-negligible probability, for

Some $\gamma = \beta \cdot \text{poly}(n)$

e.g. Gentry, Peikert, Vaik 2008 :

$q \geq \beta \cdot \sqrt{n} \cdot \omega(\log n)$

$\gamma \geq \beta \cdot \sqrt{n} \cdot \omega(\log \sqrt{n})$

$\omega(f(n))$: a fcn grows faster than $f(n)$.

or $\gamma = \tilde{O}(\sqrt{n}) \cdot \beta$

- GPV 08 also applies to ISIS with random $\vec{t}$.

4.3. Ajtai's Hash Fcn

- how SIS serves as HA to build collision-resistant hash fcn.
- hash fcn $f_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$

  $A \in \mathbb{Z}_q^{n \times m}$ random
- def $f_A(\vec{z}) = A\vec{z} \bmod q$
- Note:

  $|\{0,1\}^m| = 2^m$

  $|\mathbb{Z}_q^n| = q^n$

hash fcn takes any long → short str

⇒ requires $2^m > q^n$ ⇒ $m > n \log q$

- typically $m \approx 2n \log q$ ⇒ comp factor = 2
- Any collision $\vec{z} \neq \vec{z}'$, $f_A(\vec{z}) = f_A(\vec{z}')$

$\Rightarrow A(\vec{z}-\vec{z}') \bmod q = \vec{0}$

$\Rightarrow$ a solution to SIS with $\|\vec{z}-\vec{z}'\| \le \sqrt{m} =: \beta$

(a bit confused)

- generalization : $\{0,1\}^m$ ✓

  $\{0,1,\cdots,d-1\}^m$ for $d \ge 2$ ✓

Adv: simple, $(+, \times, \text{mod})$

Disadv: inefficient.

e.g. $q = n^2$.

$m \approx 2n \log q = 4n \log n$

size of description of f_A : $nm \log q = 8n^2 \log n$

$\Rightarrow$ we need structured lattices for efficient constructions

Leftover Hash Lemma

observe. $A \in \mathbb{Z}_q^{n \times m}$ uni rand

$\vec{z} \in \{0,1\}^m$ uni rand

$A\vec{z} \bmod q$ is statistically close to uni rand $\mathbb{Z}_q^n$

(As long as m is large enough)

$\Rightarrow$ decision variant ks prob becomes hard for large m.

Lemma 21 (LHL)

$m, n > 0$ int. prime q.

the family of hash fcns $\mathcal{H} = \{f_A : \{0,1\}^m \to \mathbb{Z}_q^n\}_{A \in \mathbb{Z}_q^{n \times m}}$

is universal.

If $m \geq n \log q - 2 + 2\log(1/\varepsilon)$ for some $\varepsilon > 0 \in \mathbb{R}$.

then:

$$\Delta\left((A, A\vec{z}), (A, \vec{u})\right) \leq \varepsilon$$

where A, $\vec{z}$, $\vec{u}$ all uni rand.

- Δ denotes statistical distance.

Review

$SD(X,Y) := \frac{1}{2} \sum_x |Pr(X=x) - Pr(Y=x)|$

or $:= \max_D |Pr(D(X)=1) - Pr(D(Y)=1)|$

proof.

$\mathcal{H}$ is universal if $P_A(f_A(\vec{z}_1) = f_A(\vec{z}_2)) = 1/|\mathbb{Z}_q^n| = q^{-n}$

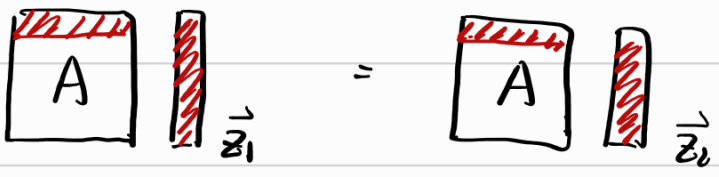
for any $\vec{z}_1 \neq \vec{z}_2$

a bit confused.

let $\vec{z}_1 \neq \vec{z}_2$ st. $A\vec{z}_1 = A\vec{z}_2$

$\vec{z}_1 \neq \vec{z}_2 \Rightarrow$ at least one coeff in them st. $z_{1k} \neq z_{2k}$

Assume $k=1$ (w/o loss of generality)



1st row: $\sum_{j=1}^m a_{1j} \cdot (z_{1j} - z_{2j}) = 0 \mod q$

take a_{11}, z_{11}, z_{21} out:

$$a_{11}(z_{11} - z_{21}) + \sum_{j=2}^m a_{1j}(z_{1j} - z_{2j}) = 0 \mod q$$

$$a_{11} \equiv (z_{21} - z_{11})^{-1} \cdot \sum_{j=2}^{m} a_{1j} (z_{1j} - z_{2j}) \mod q$$

(here: q is prime $\rightarrow$ $\mathbb{Z}_q$ is field $\rightarrow$ $\forall$ non-zero element is invertible)

Thus, a_{11} is uniquely defined by a_{1j}, $\vec{z}_1$, $\vec{z}_2$.

$\Rightarrow P(a_{11}) = \frac{1}{q}$

Apply union bound on all independent rows $\Rightarrow q^{-n}$

I think this should not be the case of union bound. Instead, it's only about the independency of rows.

$\Rightarrow$ universal property of the $\mathcal{H}$.

- Use: Dodis08, lemma 2.1

min-entropy of $U(\{0,1\}^m)$ is m

$|\mathbb{Z}_q^n| = q^n$

$\Rightarrow m \geq n \log q - 2 + 2\log(1/\varepsilon)$

e.g. if $\varepsilon = 2^{-n}$

then $m \geq n \log q - 2 + 2\log 2^n$

$= n \log q - 2 + 2n$

$2n - 2$? $2n \log q$

$(n-1) < n \leq n \log q$

$\Rightarrow m \geq 3n \log q > n \log q - 2 + 2n$ is sufficient.