The Short Integer Solution (SIS) Problem

Elena Kirshanova

MPI Reading Group

26/07/21

(based on eprint 2007/432 (GPV) and on lecture notes of D. Stehlé)

Agenda

I. SIS: definition, applications

II. SIS hardness

III. GPV signature (sketch)

Definition

$\text{SIS}_{q,m,\beta}$: (Ajtai '96)

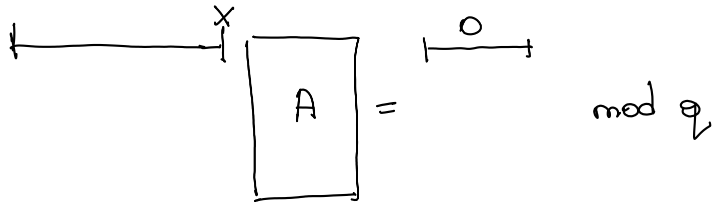
Let $n>0$, $m \geq n$, $q \geq 2$, $\beta > 0$.

$\text{SIS}_{q(n),m(n),\beta(n)}$ is given

$$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$$

The goal is to find $x \in \mathbb{Z}^m$ s.t.

1. $x^T \cdot A = 0 \mod q$
2. $0 < \|x\| \leq \beta$



We are fine with a ppt alg. $\mathcal{A}$ that solves SIS with non-negl. probality over the choice of $\mathcal{A}$ and of internal randomness.

Usually, $q = poly(n)$, $m = \Theta(n \lg n)$

SIS is average case SVP

Consider for $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

$$A^\perp = \{ b \in \mathbb{Z}^m : b^T \cdot A = 0 \bmod q \}$$

1) $A^\perp$ is a lattice

2) $\dim A^\perp = m$

3) $\det A^\perp = q^n$ (if q-prime) w.h.p.

$\Rightarrow \lambda_1 (A^\perp) = \Theta(\sqrt{m}\, q^{n/m})$

(Mink. bound)

$SIS_{q,m,\beta}$ is SVP with approx. factor $\dfrac{\beta}{\Theta(\sqrt{m}\, q^{n/m})}$ on $A^\perp$

Best known algorithm for SIS is BKZ

Constructions from SIS

I. Hash functions: $h_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$

$$x \longmapsto x^T \cdot A \bmod q$$

h_A is compressing when $n \lg q < m$.

A collision for h_A gives a solution to $SIS_{m,q,\sqrt{m}}$

$$x^T A = x'^T A \iff (x - x')^T A = 0$$

$$0 \leq \| x - x' \| \leq \sqrt{m}$$

II. Signatures: Falcon, qTesla, Dilithium ...

SIS Hardness

$$\underset{\text{(worst-case)}}{SIVP_\gamma} \leq \underset{\text{(average-case)}}{SIS_{q,m,\beta}}$$

$SIVP_\gamma$: given B - a basis of L, find $s_1 .. s_n \in L$ - lin. independent s.t. $\max_i \|s_i\| \leq \gamma \cdot \lambda_n(L)$

Thm. (Ajtai, GPV) Any ppt algorithm A solving $SIS_{q,m,\beta}$ with non-negl. probability can be used to solve $SIVP_{\gamma(n)}$ in dim. n with prob. $1-2^{-\Omega(n)}$ (over the internal randomness) if $\gamma \geq q \geq 2 \cdot n \cdot \beta \cdot \sqrt{m}$.

Some useful facts

<u>Fact 1.</u> Given a basis B of lattice L and a set $S = \{s_1 \dots s_n\}$, we can find a basis C of L, s.t. for $C = Q \cdot R$ - "QR-decomposition" of C

$\max_i r_{ii} \leq \max_i \|s_i\|$. (use LLL)

<u>Fact 2</u> We can efficiently sample from the discrete Gaussian distribution

$$\underset{\substack{\uparrow \\ \text{support}}}{D_{L}}{}_{,\underset{\substack{\uparrow \\ \text{st.dev.}}}{\sigma},\, \underset{\substack{\uparrow \\ \text{shift}}}{c}}(x) := \frac{\rho(x)}{\rho(L)} = \frac{\exp(-\pi \cdot \|x\|^2)}{\sum_{v \in L} \exp(-\pi \cdot \|v\|^2)}$$

for $\sigma \geq \sqrt{n} \cdot \max_i \|b_i\|$, where $B = \{b_i\}_{i \leq n}$ is a basis of L.

(Use Klein's sampler / GPV)

<u>Fact 3</u> Poisson Summation Formula (PSF): For every lattice L and a 'nice' f:

$$\sum_{b \in L} f(b) = \frac{1}{\det L} \sum_{\hat{b} \in \hat{L}} \hat{f}(\hat{b}), \text{ where } \hat{L} \text{ - dual to } L$$

$\hat{f}$ - Fourier transform of f

SIS Hardness Proof I.

a basis

a set of lin. indep. vectors

a hyperplane

IncIVP (B, S, H) : find $x \in L \setminus H$ s.t. $\|x\| < \frac{1}{2} \cdot \max_i \|s_i\|$

(incremental independent vector) for $\max_i \|s_i\| \geq \gamma \cdot \lambda_n(L)$

IncIVP $\leq$ SIS

SIS Hardness Proof I.

$\mathrm{IncIVP}(B, S, \mathcal{H})$: find $x \in L \setminus \mathcal{H}$ s.t. $\|x\| < \frac{1}{2} \cdot \max_i \|s_i\|$

B — a basis; S — a set of lin. indep. vectors; $\mathcal{H}$ — a hyperplane

(incremental independent vector) for $\max_i \|s_i\| \geq \gamma \cdot \lambda_n(L)$

$\mathrm{IncIVP} \leq \mathrm{SIS}$

Input: B, $S \subset L$, $\mathcal{H}$, O^{SIS} – oracle for SIS

Output: v – solution for IncIVP

1. From B and S, construct C – a basis for L
2. For $i = 1..m$:

   sample $\vec{y}_i \leftarrow D_{L,\sigma,0}$ with $\sigma = \sqrt{n} \max_i \|s_i\|$
3. Call O^{SIS} on $A = (B^{-1} \cdot Y)^T \bmod q$, where $Y = [\vec{y}_1 | \dots | \vec{y}_m]$

   Let x be the output
4. Return $v = Y \cdot x / q = \frac{1}{q} \sum x_i \cdot \vec{y}_i$.

SIS Hardness Proof II.

2. For $i = 1..m$:

   sample $\vec{y}_i \leftarrow D_{L,\sigma,0}$ with $\sigma = \sqrt{n}\max_i \|s_i\|$

3. Call O^{SIS} on $A = (B^{-1} \cdot Y)^T \bmod q$, where $Y = [\vec{y}_1 | \cdots | \vec{y}_m]$

   Let x be the output

4. Return $v = Y \cdot x / q = \frac{1}{q} \sum x_i \cdot \vec{y}_i$.

Remarks

1. $(B^{-1} \cdot Y)^T_i$ – the coordinate vector of y_i w.r.t. B mod q

   $\Rightarrow$ "x" from Step 3 is a small combination that cancels the coordinates of Y w.r.t. B

2. The reduction runs in ppt

3. The success probability can be amplified by repeating it poly(n) times

On the uniformity of A

Claim 1 $\mathcal{O}^{SIS}$ recieves on input a matrix whose distribution is within stat. distance of $2^{-\Omega(n)}$ from uniform over $\mathcal{U}(\mathbb{Z}_q^{m\times n})$

◁ Consider the first row of A, $a_1 = (B^{-1}\cdot y_1)^T \bmod q$ (the same arguments hold for the other rows, since they are independent thanks to independence of y_i's).

Let $\varphi: L \to \mathbb{Z}_q^n$ — surjective homomorphism

$y \mapsto (B^{-1}\cdot y) \bmod q$

$\Rightarrow \exists$ a bijection between $\mathbb{Z}_q^n$ and $L/\mathrm{Ker}\,\varphi = L/qL$

$\Rightarrow B^{-1}\cdot y \bmod q$ is uniform $\Leftrightarrow$ $y \bmod qL$ is uniform in L/qL.

For $\sigma \geq \eta_{2^{-n}}(qL)$, we have $\Delta(D_{L,\sigma} \bmod q, \mathcal{U}(L/qL)) \leq 2^{-\Omega(n)}$

(◁ take $b \in L/qL$: $\Pr_{b \leftarrow D_{L,\sigma}}(b) = \Pr(y \in b + qL) = \sum_{y \in b+qL} \frac{\rho_\sigma(y)}{\rho_\sigma(L)} = \frac{\rho_\sigma(b+qL)}{\rho_\sigma(L)}$ – indep. of b ∎)

∎

On the usefulness of the reduction

Claim 2 Provided $\mathcal{O}^{SIS}$ succeeds, step 4 returns v s.t.:

1. $v \in \mathcal{L}$

2. $\|v\| \le \frac{1}{q} n \cdot \beta \cdot \sqrt{m} \cdot \max_i \|s_i\|$

3. $\Pr[v \notin \mathcal{H}] = \Omega(1)$

◁ 1. $v = \frac{1}{q} \cdot Y \cdot x = \frac{1}{q} \cdot B \cdot \underbrace{B^{-1} \cdot Y}_{= A^T} \cdot x = B \cdot \underbrace{\frac{1}{q}\left(B^{-1} \cdot Y \cdot x\right)}_{\in \mathbb{Z}^n} \in \mathcal{L}$

2. $\|v\| = \frac{1}{q} \|Y \cdot x\| \le \frac{1}{q} \cdot \|x\|_1 \cdot \max_i \|y_i\| \le \frac{1}{q} \cdot \beta \cdot \sqrt{m} \cdot \max \|y_i\|$

$$\lesssim \frac{\beta}{q} \cdot \sqrt{m} \cdot \sigma \sqrt{n}$$

$$\lesssim \frac{\beta}{q} \cdot \sqrt{m} \cdot n \cdot \max_i \|s_i\|$$

3. $\mathcal{O}^{SIS}$ knows $a_i^T = B^{-1} \cdot y_i \bmod q \Leftrightarrow$ knows $y_i \bmod q\mathcal{L}$.
Conditioned on a_i, y_i is Gaussian, namely $y_i \sim D_{q\mathcal{L} + c_i, \sigma}$, where $c_i \in \mathcal{L}$ s.t. $B^{-1} \cdot c_i = a_i \bmod q$. $y_i \notin \mathcal{H}$ w.h.p. (see next slide)

Pr[v \notin H]

Claim 2.3 $\Pr_{v \leftarrow D_{L,\sigma,0}}[v \notin \mathcal{H}] = \Omega(1)$ for $\frac{\sigma}{\sqrt{2}} > \eta_{2^{-n}}(L)$ ← smoothing par-r

◁ Let w.l.o.g $\mathcal{H}$ - a hyperplane orthogonal to $(1, 0, \dots, 0)$.

$$\Pr[v \in \mathcal{H}] = \Pr[v_1 = 0] \underset{\substack{\uparrow \\ \text{Markov's ineq.}}}{\leq} \mathbb{E}[\rho(v_1)] =$$

$$= \sum_{v \in L} \rho_\sigma(v_1) \cdot \frac{\rho_\sigma(v)}{\rho_\sigma(L)} = \sum_{v \in L} \rho_{\sigma/\sqrt{2}}(v_1) \cdot \frac{\rho_\sigma(v_2) \cdot \ldots \cdot \rho_\sigma(v_n)}{\rho_\sigma(L)} =$$

$$\rho_\sigma(v) = \rho_\sigma(v_1) \cdot \rho_\sigma(v_2) \cdot \ldots \cdot \rho_\sigma(v_n)$$

$$e^{-\pi v_1^2/\sigma^2} \cdot e^{-\pi v_1^2/\sigma^2}$$

$$\overset{\text{PSF}}{=} \frac{1}{\rho_\sigma(L)} \cdot \det(\hat{L}) \cdot \frac{\sigma^n}{\sqrt{2}} \cdot \sum_{\hat{v} \in \hat{L}} \rho_{\frac{\sqrt{2}}{\sigma}}(\hat{v}_1) \cdot \ldots \cdot \rho_{\frac{1}{\sigma}}(\hat{v}_n) \leq \underbrace{\frac{\det(\hat{L}) \cdot \sigma^n}{\rho_\sigma(L)}}_{\in [1-2^{-n}, 1+2^{-n}]} \cdot \frac{1}{\sqrt{2}} \cdot \underbrace{\sum_{\hat{v} \in \hat{L}} \rho_{\frac{\sqrt{2}}{\sigma}}(\hat{v})}_{\leq (1+2^{-n}) \text{ due to the cond. on } \sigma}$$

$$x \mapsto \rho_{\sigma/\sqrt{2}}(x_1) \cdot \ldots \cdot \rho_\sigma(x_n)$$

$$\leq \frac{(1+2^{-n})}{\sqrt{2}} \Rightarrow \Pr[v \notin \mathcal{H}] \geq 1 - \frac{1+2^{-n}}{\sqrt{2}} = \Omega(1)$$

GPV signature (sketch)

Facts. 1. One can efficiently sample $A \leftarrow U(\mathbb{Z}_q^{m \times n})$ together with a short basis of $A^\perp$

2. This short basis, S_A, allows to sample from $D_{A^\perp, \sigma, c}$ for $\sigma = \max_i \|S_A[i]\| \cdot \sqrt{m}$

GPV signature = Schnorr on lattices

- KeyGen: sample A, S_A s.t. $\boxed{S_A} \cdot \underbrace{\boxed{A}}_{n} \,\big\updownarrow m = 0 \mod q$

  $sk = S_A$; $pk = A$

- Sign$(m \in \{0,1\}^*)$: 1. Compute $u = H(m) \in \mathbb{Z}_q^n$ ($H: \{0,1\}^* \to \mathbb{Z}_q^n$ - cryptographic hash fnct)

  2. Compute arbitrary $c \in \mathbb{Z}^m$ s.t. $c^T \cdot A = u^T \mod q$

  3. Sample $x \leftarrow D_{A^\perp, s, -c} + c$

  Output x as the signature

- Verify(m, x, S_A) If $\|x\| \leq \sigma\sqrt{m}$ AND $x^T \cdot A = H(m)^T \mod q$:

  Return "Accept"

  Else Return "Reject"

GPV signature (sketch)

- **KeyGen:** sample A, S_A s.t. $\boxed{S_A} \cdot \overset{\xleftrightarrow{n}}{\boxed{A}} \Big\updownarrow m = 0 \bmod q$

  $sk = S_A$; $pk = A$

- **Sign($m \in \{0,1\}^*$):**

  1. Compute $u = H(m) \in \mathbb{Z}_q^n$ ($H: \{0,1\}^* \to \mathbb{Z}_q^n$ – cryptographic hash fnct)
  2. Compute arbitrary $c \in \mathbb{Z}^m$ s.t. $c^T \cdot A = u^T \bmod q$
  3. Sample $x \leftarrow D_{A^\perp, s, -c} + c$

     Output x as the signature

- **Verify(m, x, S_A)**

  If $\|x\| \leq s\sqrt{m}$ AND $\underbrace{x^T \cdot A} = H(m)^T \bmod q$:

  Return "Accept"

  Else Return "Reject"

  $x = y + c$ for $y \in A^\perp$

  $\Rightarrow x^T \cdot A = \underset{\overset{\shortparallel}{0}}{y^T \cdot A} + c^T \cdot A = u$

GPV is EU-CMA secure in ROM provided SIS is hard.

The proof models H as Random Oracle + Forking lemma