Worst-case to Average-case Reductions

Phong Nguyên
Summary

- SIS and LWE
- A Worst-Case to Average-Case Reduction
- The discrete Gaussian distribution
The SIS Problem (1996): Small Integer Solutions

- Let \((G,+)\) be a finite Abelian group: \(G=\left(\mathbb{Z}/q\mathbb{Z}\right)^n\) in \([\text{Ajtai96}]\). View \(G\) as a \(\mathbb{Z}\)-module.

- Pick \(g_1,\ldots,g_m\) uniformly at random from \(G\).

- Goal: Find short \((x_1,\ldots,x_m)\in\mathbb{Z}^m\) s.t. \(\sum_i x_i g_i = 0\), e.g. \(\|x\| \leq m \left(\#G\right)^{1/m}\).

- This is essentially finding a short vector in a (uniform) random lattice of \(L_m(G) = \{\text{lattices } L \subseteq \mathbb{Z}^m \text{ s.t. } \mathbb{Z}^m/L \sim G\}\).
Worst-case to Average-case Reduction

- [Ajtai96]: If one can efficiently solve SIS for $G=(\mathbb{Z}/q_n\mathbb{Z})^n$ on the average, then one can efficiently find short vectors in every $n$-dim lattice.

- [GINX16]: This can be generalized to any sequence $(G_n)$ of finite abelian groups, provided that $\#G_n$ is sufficiently large $\geq n \Omega(\max(n,\text{rank}(G)))$ and $m$ too. Ex: $(\mathbb{Z}/2\mathbb{Z})^n$ is not.
Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

ABSTRACT. We give a random class of lattices in $\mathbb{Z}^n$ so that, if there is a probabilistic polynomial time algorithm which finds a short vector in a random lattice with a probability of at least $\frac{1}{2}$ then there is also a probabilistic polynomial time algorithm which solves the following three lattice problems in every lattice in $\mathbb{Z}^n$ with a probability exponentially close to one. (1) Find the length of a shortest nonzero vector in an $n$-dimensional lattice, approximately, up to a polynomial factor. (2) Find the shortest nonzero vector in an $n$-dimensional lattice $L$ where the shortest vector $v$ is unique in the sense that any other vector whose length is at most $n^c\|v\|$ is parallel to $v$, where $c$ is a sufficiently large absolute constant. (3) Find a basis $b_1, ..., b_n$ in the $n$-dimensional lattice $L$ whose length, defined as $\max_{i=1}^n \|b_i\|$, is the smallest possible up to a polynomial factor.
The SIS One-Way Function

Let $(G,+)$ be a finite Abelian group.

Pick $g_1, \ldots, g_m$ uniformly at random from $G$.

Let $f: \text{short } (x_1, \ldots, x_m) \in \mathbb{Z}^m \mapsto \sum_i x_i g_i \in G$.

$f$ is many-to-one.

Given $h = \sum_i y_i g_i \in G$, finding a short $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ s.t. $h = \sum_i x_i g_i \in G$ is as hard as SIS.
Duality

- Remember the SIS lattice:
  - $g_1, ..., g_m$ in some finite Abelian group $(G, +)$
  - $L = \{ x = (x_1, ..., x_m) \in \mathbb{Z}^m \text{ s.t. } \sum_i x_i g_i = 0 \}$

- The dual lattice of $L$ is related to the dual group $G^\vee$ of (additive) characters of $G$: morphisms from $G$ to $T = \mathbb{R}/\mathbb{Z}$

  - $L^\vee = \{ (y_1, ..., y_m) \in \mathbb{R}^m \text{ s.t. for some } s \in G^\vee, \text{ for all } i \ y_i \equiv s(g_i) \pmod{1} \}$
The LWE Problem: Learning (a Character) with Errors

- Let \( (G,+) \) be any finite Abelian group, e.g. \( G = (\mathbb{Z}/q\mathbb{Z})^n \) in [Re05].
- Pick \( g_1, \ldots, g_m \) uniformly at random from \( G \).
- Pick a random character \( s \) in \( G^\vee \).
- Goal: recover \( s \) given \( g_1, \ldots, g_m \) and noisy approximations of \( s(g_1), \ldots, s(g_m) \).
  
Ex: Gaussian noise.
Gaussian Noise over $\mathbb{R}$
Gaussian Noise over $\mathbb{R}/\mathbb{Z}$

When $\sigma$ increases, the distribution becomes uniform.
Ex: Cyclic G

- Let $G = \mathbb{Z}/q\mathbb{Z}$
- Pick $g_1, \ldots, g_m$ uniformly at random mod $q$.
- Goal: recover $s \in \mathbb{Z}$ given $g_1, \ldots, g_m$ and randomized approximations of $sg_1 \mod q, \ldots, sg_m \mod q$.
- This is exactly a randomized variant of Boneh–Venkatesan’s Hidden Number Problem from CRYPTO ’96.
Hardness of LWE

- [Regev05]: If one can efficiently solve LWE for $G = (\mathbb{Z}/q_n\mathbb{Z})^n$ on the average, then one can quantum-efficiently find short vectors in every $n$-dim lattice.

- [GINX16]: This can be generalized to any sequence $(G_n)$ of finite abelian groups, provided that $\#G_n$ is sufficiently large.
Decisional-LWE

○ Let \((G,+)\) be any finite Abelian group e.g. \(G=(\mathbb{Z}/q\mathbb{Z})^n\) in [Re05].

○ Pick \(g_1,\ldots,g_m\) uniformly at random from \(G\).

○ Pick a random character \(s\) in \(G^v\).

○ Goal: Distinguish \((g_1,\ldots,g_m,\text{noisy approximations of } s(g_1),\ldots, s(g_m))\) and uniform samples of \(G^m \times (\mathbb{R}/\mathbb{Z})^m\).
SIS and Decisional-LWE

- Suppose that one finds a short \((x_1, \ldots, x_m) \in \mathbb{Z}^m\) s.t. \(\sum_i x_i g_i = 0\).
- What can you say about \(\sum_i x_i y_i\)?
  - If \(y_1, \ldots, y_m\) are random in \(\mathbb{R}/\mathbb{Z}\).
  - If \(y_1, \ldots, y_m\) are approximations of \(s(g_1), \ldots, s(g_m)\) with a small Gaussian noise.
Variants of SIS and LWE

- Replace $\mathbb{Z}$-module by an $\mathbb{R}$-module.
- Change the distribution of
  - the LWE noise
  - the secret character
Ring Tradeoffs

- NTRU [HPS98] proposed to use special lattices: better efficiency, yet stronger hardness assumption.

- Starting with [Mi02], one can obtain ‘restricted’ worst-case to average-case reductions:
  - The worst-case now refers to a special class of lattices, e.g. ideal lattices.
M-SIS: SIS over Modules

- Let $M$ be a finite $R$-module for some ring $R$: $R=\mathbb{Z}$ in SIS. Pick $g_1, \ldots, g_m \in M$ uniformly at random.

- Goal: Find short $(x_1, \ldots, x_m) \in \mathbb{R}^m$ s.t. $\sum_i x_i g_i = 0$.

- If $\mathbb{R}^m$ is a lattice, this is finding a short vector in some random (module) sublattice of $\mathbb{R}^m$.

- Ex: NTRU used $m=2$, $R=\mathbb{Z}[X]/(X^N-1)$ and $M=\mathbb{Z}[X]/(q,X^N-1)$ but $g_1=$public key, $g_2=-1$. 
Worst-case to Average-case Reductions for Modules

- [LaSt14]: If one can efficiently solve $M$-SIS for $M=(R/qR)^d$ where $R$ is the ring of integers of a cyclotomic field, then one can efficiently find short vectors in every module lattice of $R^d$.

- This generalizes previous ideal-lattice reductions for $d=1$ [Mi02,LyMi06].

- Similar results for $M$-LWE [LaSt14] generalizing Ring-LWE hardness [LPR10].
The SIS Worst-case to Average-case Reduction
Short Lattice Vectors:
Minkowski’s Inequality

- [Minkowski]: Any $d$-dim lattice $L$ has at least one non-zero vector of norm

$$\leq 2 \frac{\Gamma(1+d/2)^{1/d}}{\sqrt{\pi}} \text{covol}(L)^{1/d} \leq \sqrt{d} \text{covol}(L)^{1/d}$$

- This is Minkowski’s inequality.
Four Proofs of Minkowski’s Inequality

- Blichfeldt’s proof: «continuous» pigeon-hole principle.
- Minkowski’s original proof: sphere packings.
- Siegel’s proof: Poisson summation.
- Mordell’s proof: pigeon-hole principle.
Mordell's Proof (1933)
Remember Blichfeldt’s Proof

- The short lattice vector is some u-\(v\) where \(u,v \in F\) for a well-chosen convex (infinite) set \(F\).

- Mordell’s proof uses a finite \(F\).
Mordell’s Proof (1933)

- For $q \in \mathbb{N}$, let $\bar{\omega} = q^{-1}L$ then $[\bar{\omega}:L] = q^d$.
  Among $>q^d$ points $v_1, \ldots, v_m$ in $\bar{\omega}$, $\exists i \neq j$ s.t. $v_i - v_j \in L$.

- There are enough points in a **large ball** of radius $r$
  ($r$ is close to Minkowski’s bound in $L$, but large for $\bar{\omega}$)

- We obtain a **short non-zero** point in $L$: norm $\leq 2r$. 
Key Point

- Mordell proved the existence of short lattice vectors by using the existence of short vectors in a special class of higher-dimensional integer lattices.

- Let distinct $v_1, \ldots, v_m \in \mathbb{L} = q^{-1}L$.

- Consider the integer lattice $L'$ formed by all $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ s.t. $\sum_i x_i v_i \in L$.

- If $m > q^d$, $\lambda_1(L') \leq \sqrt{2}$. 
An Algorithm From Mordell’s Proof

- Mordell’s proof gives an (inefficient) algorithm:
  - Need to generate $q^d$ lattice points in $\mathcal{L}$.
  - Among these exponentially many lattice points, find a difference in $L$, possibly by exhaustive search.
  - Both steps are expensive.

- [BGJ14] and [ADRS15] are more efficient randomized variants of Mordell’s algorithm: sampling over $\mathcal{L}$ may allow to sample over $L$. 

Wishful Thinking

- To apply the pigeon-hole principle, we need an exponential number $m$ of lattice vectors in $\mathcal{L}$.

- Can we get away with a small polynomial number $m$ and make the algorithm efficient? (unlike [BGJ14] and [ADRS15])

- Maybe if we could find short vectors in certain higher-dimensional random lattices.
Overlattices and Groups

- If $L$ is n-dim, $\bar{L}=q^{-1}L$ and $G=(\mathbb{Z}/q\mathbb{Z})^n$ then $\bar{L}/L \cong G$.
- There is an exact sequence:

\[ 0 \rightarrow L \overset{1}{\rightarrow} \bar{L} \overset{\varphi}{\rightarrow} G \rightarrow 0 \]

- $L=\text{Ker } \varphi$ where $\varphi$ is efficiently computable: which $\varphi$?
- Let $v_1,\ldots,v_m \in \bar{L}$ and define $g_1,\ldots,g_m \in G$ by $g_i=\varphi(v_i)$.

\[ \sum_i x_i g_i = 0 \text{ for } (x_1,\ldots,x_m) \in \mathbb{Z}^m \text{ iff } \sum_i x_i v_i \in L. \]
Fourier analysis shows that if \( v_1, \ldots, v_m \in \mathcal{L} \) are chosen from a suitable (short) distribution, \( g_i = \varphi(v_i) \) has uniform distribution over \( G \).

Any probability mass function \( f \) over \( \mathcal{L} \) s.t. for any \( x \in \mathcal{L} \), \( \sum_{y \in \mathcal{L}} f(x+y) \approx 1/\#G \).

Ex: discrete Gaussian distribution.

This is a key step: transforming a worst-case into an average-case.
Remember SIS

- Let \((G,+)\) be a finite Abelian group: \(G = (\mathbb{Z}/q\mathbb{Z})^n\) in [Ajtai96]. View \(G\) as a \(\mathbb{Z}\)-module.
- Pick \(g_1,\ldots,g_m\) uniformly at random from \(G\).
- Goal: Find short \((x_1,\ldots,x_m) \in \mathbb{Z}^m\) s.t. \(\sum_i x_i g_i = 0\), e.g. \(\|x\| \leq m (\#G)^{1/m}\).
- This is essentially finding a short vector in a (uniform) random lattice of \(L_m(G) = \{ \text{lattices } L \subseteq \mathbb{Z}^m \text{ s.t. } \mathbb{Z}^m/L \sim G \}\).
Worst-to-average Reduction from Mordell’s Proof

- Sample short \( v_1, \ldots, v_m \in \mathbb{L} \) from a suitable distribution, so that \( g_i = \varphi(v_i) \) has uniform distrib. over \( G = (\mathbb{Z}/q\mathbb{Z})^n \).

- Call the SIS-oracle on \( (g_1, \ldots, g_m) \) to find a short \( x = (x_1, \ldots, x_m) \in \mathbb{Z}^m \) s.t. \( \sum_i x_i g_i = 0 \) in \( G \), i.e. \( \sum_i x_i v_i \in \mathbb{L} \).

- Return \( \sum_i x_i v_i \in \mathbb{L} \).
Generalized SIS Reduction

- The SIS reduction is based on this crucial fact: If $B$ is a reduced basis of a lattice $L$, then $q^{-1}B$ is a reduced basis of the overlattice $\mathcal{L} = q^{-1}L$.

- But if $G$ is an arbitrary finite Abelian group, we need to find a reduced basis of some overlattice $\mathcal{L} \supseteq L$ s.t. $\mathcal{L}/L \cong G$, so that we can sample short vectors in $\mathcal{L}$. 
In classical lattice reduction, we try to find a good basis of a given lattice.

In structural lattice reduction [GINX16], given a lattice $L$ and a (sufficiently large) finite Abelian group $G$, we find a good basis of some overlattice $\mathcal{L}$ s.t. $\mathcal{L}/L \cong G$. 
Easy Cases

- If $G = (\mathbb{Z}/q\mathbb{Z})^n$, any basis $B$ of a full-rank lattice $L$ in $\mathbb{Z}^n$ can be transformed into a basis $q^{-1}B$ of $\mathcal{L} = q^{-1}L$, which is $q = \#G^{1/n}$ times shorter.

- If $G = \mathbb{Z}^n/L$, the canonical basis of $\mathcal{L} = \mathbb{Z}^n$ is a short basis, typically $\#G^{1/n}$ times shorter than a short basis of $L$. 
Though lattices are infinite, there is a natural probability distribution over lattice points, introduced by [Ba1993] for transference.

This Gaussian measure was implicitly used in [Klein00]'s randomized variant of Babai's nearest-plane algorithm to solve BDD.

[Regev2005] noted that the Gaussian measure could sometimes be sampled.

[GPV2008] rediscovered [Klein00] and showed that it samples from the Gaussian measure.
Gaussian Measure

- Center $c$, parameter $s$
- Mass of $x \in L$ proportional to
  \[\rho_{s,c}(\vec{x}) = e^{-\pi \| \frac{\vec{x} - \vec{c}}{s} \|^2}\]
- The distribution is independent of the basis.
- Introduced in [Ba93], then used in cryptography in [Cai99, Regev03, MiRe04, ...]
Beyond the smoothing parameter, the discrete Gaussian distribution behaves like a continuous Gaussian.