MIT 6.829: 6.876 Advanced Topics in Cryptography: Lattices	Fall 2015
Lecture 11	
Lecturer: Vinod Vaikuntanathan	*Student: Tianren Liu*

1 Overview

- Worst-case to average-case reduction

  Worst-case problems are typically harder than average-case problems. While if there is worst-case to average-case reduction, you are able to solve the problem in worst-case if you can solve a problem in average case.

  An example of worst-case to average-case reduction is RSA. Assume there is an black box reverse RSA, i.e. you known N, e, the box output $m^{e^{-1} \mod \phi(N)}$ on input m. While the box is only guaranteed to work w.h.p. on random input m. Then given m, your could query the box on input $m' = m \cdot r^e$ for random r, then the box should output $m^{e^{-1}} \cdot r$ with high probability.

- Cryptography constructions (One-way functions, CRHFs)

2 Reduce worst-case $\mathsf{SIVP}_{\tilde{O}(n)}$ to average-case SIS (Short Integer Solutions) [MR07]

Definition 2.1 (Search SIVP_γ)**.** Given a lattice $\mathcal{L}$, find n linear independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in L such that $\|\mathbf{v}_i\|_2 \leq \gamma\lambda_n$.

Definition 2.2 ($\mathsf{SIS}(n, m, q, \beta)$)**.** Given $A \in \mathbb{Z}_q^{n\times m}$, find $\mathbf{e} \in \mathbb{Z}_q^m$ s.t.

1. $A\mathbf{e} = 0$
2. $\mathbf{e} \neq 0$
3. $\|\mathbf{e}\|_2 \leq \beta$

Moreover, SIS is typically considered as an average-case problem. An oracle solving SIS would output a short solution w.h.p. given uniform random input A.

We choose parameter $m > \frac{n \log q}{\log(\beta+1/2)}$ so that a short solution is guaranteed.

Remark.
- Parameter: When $m < n$, the SIS problem is trivial. The case when $n < m < n \log n$ is similar to LWE.
- We could define f_A by $f_A(\mathbf{e}) = A\mathbf{e} \mod q$, f_A is "many-to-one" under such parameter.

- SIS is a lattice problem. The set $\Lambda^{\perp}(A) = \{\mathbf{e} : A\mathbf{e} = 0 \mod q\}$ is an integer lattice and A is the "parity check" matrix. SIS problem is to find a non-zero short vector in the lattice.
- SIS can be defined more generally on a Abelian group $\mathbb{G}$. In $\mathsf{SIS}_{\mathbb{G}}$, given $a_1, \ldots, a_m \in \mathbb{G}$, find short vector $(e_1, \ldots, e_m) \in \mathbb{Z}^m$ such that $\sum e_i a_i = 0$.
- Another generalization is ISIS (Inhomogenous SIS), given $A, \mathbf{b}$, find $\mathbf{e}$ such that $A\mathbf{e} = \mathbf{b} \mod q$.

Theorem 2.1. *There is a polytime reduction from* $\mathsf{SIVP}_{\tilde{O}(n)}$ *to average-case* $\mathsf{SIS}_{n,m,q,\beta}$*, where* $q = \Omega(n^2), \beta = O(\sqrt{m}), m \approx n \log q$.

An important concept in the proof is Gaussian distribution. In n-dim Gaussian, $\rho_s(\mathbf{u}) \propto e^{-\frac{\|\mathbf{u}\|^2}{s^2}}$. Consider we pick a random lattice, then add a Gaussian noise with variance s. (Formally, we should sample from Gaussian distribution and modulo parallelepiped.) If $s \ll \lambda_1$, the resulting distribution should concentrate around the lattice points. If $s \gg \lambda_1$, then the Gaussian distribution rooted at two neighbor lattice points "merge together". If s is sufficiently large, then the distribution is close to uniform distribution.

To quantify this idea, we define the smoothing parameter η_ε as in [MR07]

Definition 2.3 (Smoothing parameter $\eta_\varepsilon(\mathcal{L}(B))$)**.** The smoothing parameter of lattice $\mathcal{L}(B)$ of error ε is the minimum variance of Gaussian, such that its modulo over parallelepiped $P(B)$ is ε-close to uniform.

$$\eta_\varepsilon(\mathcal{L}(B)) = \inf\{s : \Delta_{\text{sd}}(\mathcal{N}(0, s^2) \mod P(B), \mathcal{U}_{P(B)}) \leq \varepsilon\}$$

Theorem 2.2 (Banaszczyk [Ban95, Pei08])**.** *For every lattice,*

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\log(1/\varepsilon) + \log n} \cdot \lambda_n$$

Proof of Theorem 2.1. The reduction is

Given basis $B \in \mathcal{Z}^{n \times n}$, (and assume that λ_n is known)

1. Choose $\mathbf{x}_1, \ldots, \mathbf{x}_n$ from n-dimensional Gaussian $\mathcal{N}(0, s^2)$ such that $s \geq \eta_\varepsilon(L)$
2. $\mathbf{y}_i = \mathbf{x}_i \mod P(B)$

Then we known $\mathbf{y}_i$ should satisfies (close to) uniform distribution in $P(B)$.

We consider the sup-lattice $\mathcal{L}(\frac{1}{q}B) = \{\mathbf{v}/q : \mathbf{v} \in \mathcal{L}(B)\}$, which is q^n times more dense then $L(B)$. Round $\mathbf{y}_i$ to a vector $\mathbf{z}_i$ in this sup-lattice, and let $\mathbf{a}_i$ be the coefficient of the lattice point under base $\frac{1}{q}B$.

3. $\mathbf{a}_i = \lceil q \cdot B^{-1}\mathbf{y}_i \rfloor$, $\mathbf{z}_i = \frac{1}{q}B\mathbf{a}_i$

Then $\mathbf{z}_i = \frac{1}{q}B\mathbf{a}_i$ is the lattice point in $\mathcal{L}(\frac{1}{q}B)$, and it's close to $\mathbf{y}_i$. Moreover, $\mathbf{a}_i$ should be (almost) uniform random in $\mathbb{Z}_q$.

4. Feed $(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ as input to the SIS oracle, get $(e_1, \ldots, e_m)$.

5. $\sum e_i(\mathbf{x}_i - \mathbf{y}_i + \mathbf{z}_i)$ is a short lattice vector.

Correct: Vector $\sum e_i(\mathbf{x}_i - \mathbf{y}_i + \mathbf{z}_i)$ is a lattice point. $\sum e_i(\mathbf{x}_i - \mathbf{y}_i)$ is a lattice point because $\mathbf{x}_i - \mathbf{y}_i$ is a lattice point; and $\sum e_i \mathbf{z}_i$ is a lattice point because $\sum e_i \mathbf{a}_i = 0 \mod q$

$$\begin{aligned} & \sum e_i \mathbf{a}_i = 0 \mod q \\ \implies & \sum e_i \frac{1}{q} \mathbf{a}_i = 0 \mod 1 \\ \implies & \sum e_i \frac{1}{q} B\mathbf{a}_i = 0 \mod P(B) \\ \implies & \sum e_i \mathbf{z}_i = 0 \mod P(B) \end{aligned}$$

Short: Vector $\sum e_i(\mathbf{x}_i - \mathbf{y}_i + \mathbf{z}_i)$ is a short vector.

$$\begin{aligned} \|\mathbf{v}\| &\le \|\sum e_i \mathbf{x}_i\| + \|\sum e_i(\mathbf{y}_i - \mathbf{z}_i)\| \\ &\le \|e\| \cdot \|\mathbf{x}\| + \frac{n \max_i \|\mathbf{b}_i\|}{q} \\ &\le \beta \cdot s\sqrt{n} + \frac{n \max_i \|\mathbf{b}_i\|}{q} \end{aligned}$$

The problem is that $\|\mathbf{b}_i\|$ might be so large that the output $\mathbf{v}$ is not a short vector. In such case, $\mathbf{v}$ is shorter than $\max_i \|\mathbf{b}_i\|$ (if q is sufficiently large), then we could use $\mathbf{v}$ to update the basis so that we'll get a shorter basis.

Set $q \ge n^2$. If $\max_i \|\mathbf{b}_i\| > \tilde{\Omega}(n\lambda_n)$, we get $\mathbf{v}$ that is smaller than $\max_i \|\mathbf{b}_i\|$. Use it to update the basis and reduce $\max \|\mathbf{b}_i\|$. Repeat such process many times until $\|\mathbf{b}_i\| = \tilde{O}(n\lambda_n)$, then $\|\mathbf{v}\| \approx O(\beta\sqrt{mn})$.

Non-zero and cheat: The above analysis does not rule out the possibility that $\mathbf{v} = 0$. We are solving Search SIVP_λ, we are looking for n linear independent lattice points, while the procedure might always output lattice points from a subspace. Also, when $\max_i \|\mathbf{b}_i\|$, we use $\mathbf{v}$ to update the basis, while if $\mathbf{v}$ is limited in a subspace, e.g. the space spanned by $\mathbf{b}_1$, then $\mathbf{v}$ can not be used to improve the basis. In either case, we hope $\mathbf{v}$ is not limited in any subspace. We relies on randomness to solve the problem. E.g. if $\mathbf{v}$ is uniformly sampled from all lattice points that $\|\mathbf{v}\| \le \tilde{O}(\beta\sqrt{mn})$, then all the problems are fixed.

Notice that in our procedure, step 3 and 4, $\mathbf{x}_i$ is never used, and $\mathbf{y}_i$ is their best knowledge about $\mathbf{x}_i$. Given $\mathbf{y}_i = \mathbf{x}_i \mod P(B)$, vector $\mathbf{x}_i - \mathbf{y}_i$ satisfies discrete Gaussian distribution, which is a distribution over lattice $\mathcal{L}$ such that $\rho_s(\mathbf{u}) \propto e^{\frac{\|\mathbf{u}\|^2}{s^2}}$.

The procedure outputs $\mathbf{v} = \sum e_i(\mathbf{x}_i - \mathbf{y}_i) + \sum e_i \mathbf{z}_i$. Given the values used in step 3 and 4, $\sum e_i \mathbf{z}_i$ is a fixed number, while $\sum e_i(\mathbf{x}_i - \mathbf{y}_i)$ is sum of discrete Gaussian, which satisfies discrete Gaussian with standard deviation $\|\mathbf{e}\|_2 s$. These provide sufficient randomness to fix the problems mentioned above. □

3 Reduce SAT to inverting OWF? (Is $\mathsf{SAT} \leq \mathsf{OWF}$?)

Question: we are given an oracle inverting a family of one-way functions. Could you use it to solve SAT in polynomial time?

Consider a special case where the family is consist of permutations. Any language that can be reduced to inverting one-way permutation is in $\mathsf{NP} \cap \mathsf{coNP}$. So SAT can not be reduce to inverting one-way permutations unless polynomial hierarchy collapses.

Slightly more generally, if a language can be reduce to inverting an one-way functions family that is regular (or size-verifiable). Then the language is in $\mathsf{AM} \cap \mathsf{coAM} \subsetneq \mathsf{NP}$ [BB15]. This rule out the probability that you can reduce SAT to worst-case inverting regular one-way functions.

Another negative result: NP-hard problems cannot be reduce to arbitrary one-way functions family, if the reduction is non-adaptive (or constant-round adaptive) [HMX10].

What we are looking for is an reduction from SAT to average-case inverting an one-way functions family. We have not ruled out this probability, but we known the OWF family must not be regular or size-verifiable, and the reduction must be (heavily) adaptive.

We can easily construct a "one-way functions family", inverting which in worst-case implies solving SAT. While the worst-case hardness is not a useful guarantee in cryptography. The reduction from SIVP to SIS is extremely interesting because it reduce inverting a one-way function in worst-case to an average-case problem.

References

[Ban95] Wojciech Banaszczyk. Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$. *Discrete & Computational Geometry*, 13(1):217–231, 1995.

[BB15] Andrej Bogdanov and Christina Brzuska. On basing size-verifiable one-way functions on np-hardness. In *Theory of Cryptography*, pages 1–6. Springer, 2015.

[HMX10] Iftach Haitner, Mohammad Mahmoody, and David Xiao. A new sampling protocol and applications to basing cryptographic primitives on the hardness of np. In *Computational Complexity (CCC), 2010 IEEE 25th Annual Conference on*, pages 76–87. IEEE, 2010.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.

[Pei08] Chris Peikert. Limits on the hardness of lattice problems in ℓ_p norms. *Computational Complexity*, 17(2):300–351, 2008.