6.876 Advanced Topics in Cryptography: Lattices	September 28, 2015
Lecture 6	
Lecturer: Vinod Vaikuntanathan	*Scribe: Gaurav Singh*

The following four problems look different, but we can use one technique to solve all of them.

1. (Complexity) $GapSVP_{\sqrt{\frac{n}{\log n}}} \in coAM$
2. (Algorithms) SVP_1 can be solved in $2^{O(n)}$ randomized time.
3. (Cryptography) Worst-case to average case results.
   (a) $GapSVP_n \leq SIS$
   (b) $GapSVP_n \leq LWE$

Here we show the first one. We start with a quick review of definitions.

Definition 1 ($GapSVP_\gamma$)**.** $GapSVP_\gamma$ is a promise problem, where inputs are guaranteed to be either a YES or NO instance. Here, these are,

- YES: $(\mathcal{L}, s)$ such that $\lambda_1(\mathcal{L}) \leq s$.
- NO: $(\mathcal{L}, s)$ such that $\lambda_1(\mathcal{L}) > \gamma s$.

Definition 2 (AM)**.** An Arthur-Merlin Protocol for a language L consists of an unbounded M and a polynomial time A with a source of randomness r, such that for an input x, and a transcript of messages between A and M, after which A accepts or rejects, we have,

- If $x \in YES$, then A accepts with probability 1.
- If $x \in No$, then for any A, $\mathbb{P}[A \text{ accepts}] \leq \frac{1}{3}$.

Note that $GapSVP_\gamma \in NP$. To see this, on a YES instance, a short vector is a certificate for this property.

Theorem 1 (Goldreich-Goldwasser 2000)**.** *For $\gamma = \omega(\sqrt{\frac{n}{\log n}})$, $GapSVP_\gamma \in coAM$.*

Proof. We will instead prove that $coGapSVP_\gamma \in AM$. The idea behind the protocol for this is the following. The verifier picks either the target point or a lattice point, and sends a point close to it to the prover. The prover then responds with a guess as to whether the point came from a lattice point or the target point, and if they are close together, the prover has some chance of being wrong. See Figures 1 and 2 for a visual sketch of the idea.

More precisely, our protocol is the following. Given a basis $\mathbf{B}$, and a target point t, the verifier picks a random $x \in B(0, \frac{\gamma}{2})$, and $b \in \{0, 1\}$, and sends $z_b = x + bt \mod \mathcal{P}(\mathbf{B})$, where $\mathcal{P}(\mathbf{B})$ is the fundamental parallelpiped of $\mathbf{B}$. Then, the prover sends b' to the verifier, and the verifier accepts if $b = b'$.

Now, we just need to show that this protocol is complete and sound. To see it's complete, if $dist(t, \mathcal{L}(\mathbf{B})) > \gamma$, then $B(0, \frac{\gamma}{2}) \cap B(t, \frac{\gamma}{2}) = \emptyset$. Then the prover can always distinguish z_0 from z_1, and with probability 1, the verifier accepts.

For soundess, we want to show that with probability at most $1 - \frac{1}{poly(n)}$ can z_0 and z_1 be confused. If this is the case, with at least an inverse polynomial probability, the verifier rejects. This is equivalent to bounding the volume of $|B(0, \frac{\gamma}{2}) \cap B(t, \frac{\gamma}{2})|$. We can bound this by a cylinder. This gives, using the fact that the volume of a unit n-ball is $\frac{\pi^{n/2}}{\Gamma(n/2+1)}$, and Stirling's approximation,

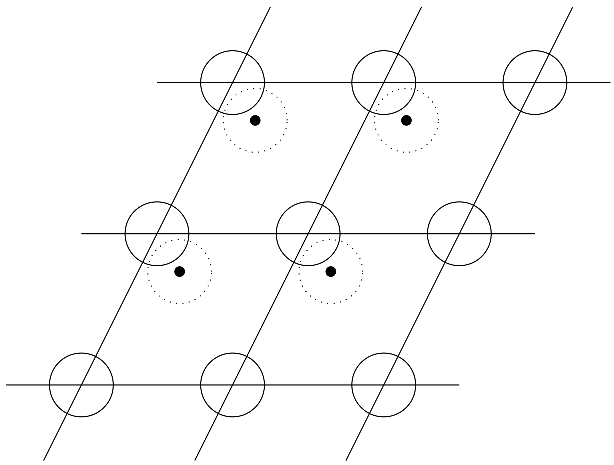

Figure 1: The target is close to the lattice.

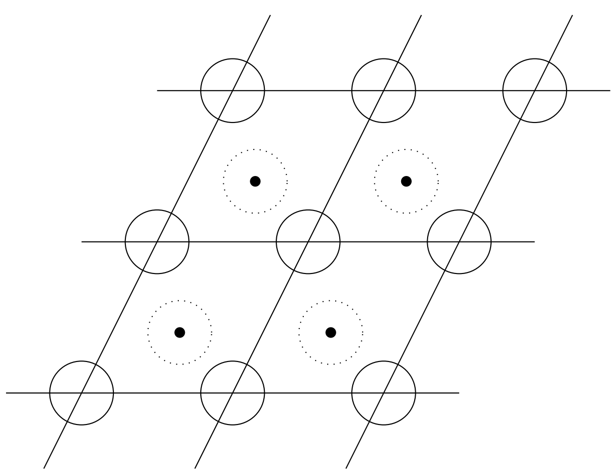

Figure 2: The target is far from the lattice.

$$
\begin{aligned}
\frac{|B(0,\frac{\gamma}{2})\cap B(t,\frac{\gamma}{2})|}{|B(0,\frac{\gamma}{2})|} &\geq \frac{|t|\left(\frac{\pi^{(n-1)/2}}{\Gamma\left(\frac{n-1}{2}+1\right)}\right)\left(\sqrt{\left(\frac{\gamma}{2}\right)^2-|t|^2}\right)^{n-1}}{\left(\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\right)\left(\frac{\gamma}{2}\right)^n} \\
&= \frac{\Gamma\left(\frac{n}{2}+1\right)}{\sqrt{\pi}\Gamma\left(\frac{n-1}{2}+1\right)}\left(\frac{2|t|(\gamma^2-4|t|^2)^{(n-1)/2}}{\gamma^n}\right) \\
&= \frac{C\sqrt{2\pi(n/2+1)}\left(\frac{n/2+1}{e}\right)^{n/2+1}}{\sqrt{\pi}c\sqrt{2\pi((n-1)/2+1)}\left(\frac{(n-1)/2+1}{e}\right)^{(n-1)/2+1}}\left(\frac{2|t|(\gamma^2-4|t|^2)^{(n-1)/2}}{\gamma^n}\right) \\
&\approx \frac{c'\sqrt{n}|t|(\gamma^2-4|t|^2)^{(n-1)/2}}{\gamma^n} \\
&= c'\sqrt{n}\frac{|t|}{\gamma}\left(1-4\left(\frac{|t|}{\gamma}\right)^2\right)^{(n-1)/2} \\
&\geq c'\sqrt{n}\sqrt{\frac{\log n}{n}}\left(1-\frac{4\log n}{n}\right)^{(n-1)/2} \\
&= c'\sqrt{\log n}\left(1-\frac{4\log n}{n}\right)^{(n-1)/2} \\
&\approx c'\sqrt{\log n}e^{-c_1\log n} \\
&\approx \frac{1}{poly(n)}
\end{aligned}
$$

This means that there is at least an inverse polynomial probability that a random point could have either $b = 0$ or $b = 1$, which means that this protocol is also sound.

□

References

[1] . Goldreich and S. Goldwasser. On the limits of nonapproximability of lattice problems. J. Comput. System Sci., 60(3):540563, 2000.