Lattice-based Cryptanalysis:

Mar-17, 2011

I Simultaneous Diophantine approximation (SDA): Lagarias '82

* Diophantine Approx: Given a real x, approximate it as a/b (with integer a, b), such that $|x - a/b| \ll \frac{1}{2b}$

* Simultaneous D.A: Given many x_i's, approximate all with the same approximate-common-denominator $\{\frac{a_i}{b}\}$ s.t. $|\frac{a_i}{b} - x_i| \ll \frac{1}{2b}$

* If the x_i's are rational then there is an exact solution $x_i = a_i/b$ (b is the LCM of all the denominators) but we often want to approximate with denominator $\ll b$.

* Definition: Let $\{x_i \equiv \frac{a_i}{b} \mid a_i, b \in \mathbb{Z},\ i = 1, 2, \dots n\}$ be an instance of SDA. We say that an approximate-common-denominator q is of quality (ε, δ) if $q \neq 0$, $q \in \mathbb{Z}$ and the following conditions hold
  - $q \le \varepsilon b$, and
  - $q \cdot x_i$ is within $\delta/2$ of an integer for all $i = 1, 2, \dots n$

  (namely $\exists p_i$ such that $\left|\frac{a_i}{b} - \frac{p_i}{q}\right| \le \delta/2q$)

* Consider the lattice spanned by columns of $B_{(n+1)\times(n+1)}$ (where c is a parameter).

$$B = \begin{pmatrix} c & & & & \\ a_1 & b & & & \\ a_2 & & b & & \\ \vdots & & & \ddots & \\ a_n & & & & b \end{pmatrix}$$

Note: $\det(B) = b^n \cdot c$, so by Minkowsky we know that $\Lambda(B)$ has nonzero vectors of length $\le \sqrt{n+1} \cdot \det(B)^{1/n+1} = \sqrt{n+1} \cdot b \cdot \left(\frac{c}{b}\right)^{1/n+1}$.

Heuristically we expect $\Lambda(B)$ to have exponentially many vectors (in n) of length $\le poly(n) \cdot b \cdot \left(\frac{c}{b}\right)^{1/n+1}$, and for "random" SDA instance we expect no vectors of length $\le b \cdot \left(\frac{c}{b}\right)^{1/n+1} / poly(n)$

* Claim: From any vector in $\Lambda(B)$ of length $0 \lneq l \lneq b$ we can compute efficiently an approx-common-denominator q of quality (ε, δ) with $\varepsilon \le l/b \cdot c$, $\delta \le 2l/b$

Proof: Let $\vec{x} \in \Lambda(B)$, $0 \neq \|\vec{x}\| \lneq b$, and we write $\vec{x} = B\vec{\alpha}$ with $\vec{\alpha}$ an integer vector

$$\vec{x} = \begin{pmatrix} c & & & \\ a_1 & b & & \\ \vdots & & \ddots & \\ a_n & & & b \end{pmatrix} \underbrace{\begin{pmatrix} q \\ -p_1 \\ \vdots \\ -p_n \end{pmatrix}}_{\vec{\alpha}} = \begin{pmatrix} cq \\ qa_1 - p_1 b \\ \vdots \\ qa_n - p_n b \end{pmatrix} = b \begin{pmatrix} c\,q/b \\ q\frac{a_1}{b} - p_1 \\ \vdots \\ q\frac{a_n}{b} - p_n \end{pmatrix}$$

Note that we cannot have $q=0$, or else we get $\|x\| \geq \max_i \{|p_i|\} \cdot b$ and since the p_i's are integers and $\|x\| \lneq b$ then it must be that all the p_i's are zero (which is a contradiction).

- Hence we have $cq \leq \ell$ so $\varepsilon = q/b \leq \ell/b\cdot c$
- Also, for all i, the distance from $q \cdot \frac{a_i}{b}$ to the nearest integer is at most $|q\frac{a_i}{b} - p_i| \leq \ell/b$, namely $\delta \leq \frac{2\ell}{b}$ ☒

Note: If we want to set $\varepsilon = \delta$ then we need $c = 1/2$, but usually (ε, δ) come from the application and then we set $c = \delta/2\varepsilon$.

Claim: From any approx.-common-denominator which is (ε, δ)-good we can compute a vector $0 \neq \vec{x} \in \Lambda(B)$ of length at most
$\|\vec{x}\| \leq b \cdot \sqrt{(c\cdot\varepsilon)^2 + n \cdot \delta^2} \leq b(c\varepsilon + \sqrt{n}\,\delta)$.

Proof is essentially the same as above. ☒

* Hence there is basically 1-1 correspondence between "good" approx.-common-denominators and "short" vectors in $\Lambda(B)$.

Note: This is an easy example of how lattice-based algorithms work: We look for ways to cast the problem at hand as consisting of linear relations with integer coefficients and finding small solutions.

Using SDA to solve approximate-GCD

* We have parameters $\rho \ll n \ll \gamma$. We are given as input $\{ w_i = q_i p + r_i \mid i = 0, 1, \dots, n \}$ where $p \in_R [2^{n-1}+1, 2^n - 1]$, p odd
  $q_i \in_R [2^{\gamma-1}, 2^\gamma - 1]$, $r_i \in_R [-2^\rho + 1, 2^\rho - 1]$.

  We can assume w.l.o.g. that $w_0 > w_i$ for all $i \Rightarrow q_0 \geq q_i$.
* Construct the SDA instance $\{ x_i = w_i / w_0 \mid i = 1, \dots, n \}$

Claim: q_0 is an approx.-common-denominator of quality (ε, δ) with $\varepsilon \le 2^{-n+1}$ and $\delta \le 2^{\rho - n + 3}$

Proof: $\varepsilon = q_0 / w_0 = \dfrac{q_0}{q_0 p + r_0} = \dfrac{q_0}{q_0 (p + r_0/q_0)} \le \dfrac{1}{p-1} \le 2^{-n+1}$.

To bound δ, note that

$$q_0 \cdot \frac{w_i}{w_0} = q_0 \frac{q_i p + r_i}{q_0 p + r_0} = \frac{q_i p + r_i}{p + r_0/q_0} = \frac{q_i (p + r_0/q_0) - \frac{q_i}{q_0} r_0 + r_i}{p + r_0/q_0} = q_i + \frac{r_i - q_i/q_0 \cdot r_0}{p + r_0/q_0}$$

hence the distance between $q_0 \cdot \frac{w_i}{w_0}$ and the nearest integer is

$\frac{q_i}{q_0} \le 1$

$$\delta/2 = \left| \frac{r_i - q_i/q_0 \, r_0}{p + r_0/q_0} \right| \le \frac{|r_i| + |r_0|}{p-1} \le \frac{2^{\rho+1}}{2^{n-1}} = 2^{\rho - n + 2}$$ ⊠

* We therefore use parameter $c = \delta / 2\varepsilon = \dfrac{2^{\rho-n+3}}{2 \cdot 2^{-n+1}} = 2^{\rho+1}$ for the lattice

$$B = \begin{pmatrix} 2^{\rho+1} & & & \\ w_1 & w_0 & & \\ \vdots & & \ddots & \\ w_n & & & w_0 \end{pmatrix}$$

$\det(B) = w_0^{n+1} \cdot \dfrac{2^{\rho+1}}{w_0}$, if this was a "random instance" then we expect to find in $\Lambda(B)$ vectors of size $\sim w_0 \left(\dfrac{2^{\rho+1}}{w_0} \right)^{1/n+1} \cdot \sqrt{n+1}$

However, the vector corresponding to q_0 has size $\le \sqrt{n+1} \cdot q_0 \cdot 2^{\rho+1}$

Q1: When do we expect that the vector corresponding to q_0 be the shortest nonzero vector in $\Lambda(B)$?

A: When n is large enough so that $q_0 \cdot 2^{\rho+1} \ll w_0 \cdot \left(\dfrac{2^{\rho+1}}{w_0} \right)^{1/n+1}$

Recall that $q_0 \sim 2^\gamma$, $w_0 \sim 2^{\gamma+n}$, this means that we need

$$2^{\gamma+\rho+1} \ll 2^{\gamma + n + ((\rho+1-\gamma)/n+1)} \iff \cancel{\gamma} + \rho + 1 \ll \cancel{\gamma} + n + \frac{\rho+1-\gamma}{n+1}$$

$$\iff n+1 \gg \frac{\gamma - \rho - 1}{n - \rho - 1} \approx \gamma / n$$

* If we have enough samples ($n \gg \gamma/\eta$) the the vector corresponding to q_0 will be the shortest nonzero vector in $\Lambda(B)$. We can then hope that running LLL on B will recover this vector, and thereby also q_0 (and the secret p).

Q2: Will this attack work?

A: Depends on the sizes of η and γ (recall $p \sim 2^{\eta}$, $q_i \sim 2^{\gamma}$).

Example-1: Assume that we set $\gamma = \eta^2$, and $n = 2\gamma/\eta = 2\eta$

- The smallest vector in $\Lambda(B)$ is the one corresponding to q_0 of size $\sim \sqrt{2\eta} \cdot 2^{\gamma+\rho}$
- All the vectors in $\Lambda(B)$ that are not multiples of the shortest are of size $\sim \sqrt{2\eta} \cdot w_0 \cdot \left(\frac{2^{\rho}}{w_0}\right)^{1/2\eta} \sim \sqrt{2\eta} \cdot 2^{\gamma+\eta+((\rho-\gamma)/2\eta)} = \sqrt{2\eta} \cdot 2^{\gamma+\eta-\frac{\eta}{2}+\frac{\rho}{2\eta}}$

$$\gtrsim \sqrt{2\eta} \cdot 2^{\gamma+\eta/2}$$

- Using LLL-like algorithm with approximation factor $\leq 2^{n/8} = 2^{\eta/4}$ we can find a vector in $\Lambda(B)$ of size at most
$2^{\eta/4} \cdot \sqrt{2\eta} \cdot 2^{\gamma+\rho} = \sqrt{2\eta} \cdot 2^{\gamma+\eta/4+\rho} \lneq \sqrt{2\eta} \cdot 2^{\gamma+\eta/2}$
Hence this must be a multiple of the vector corresponding to q_0.
Then we can find the vector itself, and therefore q_0 and p.

Example 2: Set $\gamma = \eta^3$, and still $n = 2\gamma/\eta = 2\eta^2$

- Now any algorithm with approximation factor $2^{\epsilon n} = 2^{2\epsilon\eta^2}$ will only be able to find vectors of size
$\sqrt{2\eta} \cdot 2^{\gamma+2\epsilon\eta^2+\rho} \gg \sqrt{2\eta} \cdot 2^{\gamma+\eta/2}$
Hence it will almost surely find on of the exponentially many auxiliary vectors, and not the one corresponding to q_0

Tracing through the parameters, the "safe region" is $\gamma = \omega(\eta^2)$.