Coppersmith's Method: finding small solutions to polynomial eqn's.

* Example: Suppose you wanted to use RSA encryption with exponent 3, and moreover you put the plaintext as the low-order bits, and put an n-bit random value as the high-order bits (e.g. $n=128$ or $n=256$). Namely, $Enc_N(x) = (x + 2^{k-n} \cdot r)^3 \bmod N$ (k is the bit-length of N). We want to show that if n is too small wrt. k then this is not semantically secure.

The attacker is given a candidate x and an encrytion $c \overset{?}{=} (x + 2^{k-n} \cdot r)^3 \bmod N$, and it wants to check whther or not there exists an n-bit solution r. Namely, an n-bit root of the polynomial

$$f_c(z) = z^3 + 3\left(\frac{x}{2^{k-n}}\right) z^2 + 3\left(\frac{x}{2^{k-n}}\right)^2 z + \left(\frac{x}{2^{k-n}}\right)^3 \bmod N$$

* More generally, we are given a degree-d polynomial

$$F(z) = \sum_{i=0}^{d} f_i z^i \pmod{M}$$

and a bound X, and we want to find a root of $F(z)$ modulo N of size $|z| < X$, if one exists.

* Simple case: f has small coefficients. Suppose that $F(X) < M$ over the integers. In this case $F(z) = 0 \bmod M$ with $0 \le z \le X$ iff $F(z) = 0$ over the integers (or reals), so we can solve for it (e.g. using Newton's method).

* Beyond the simple case, Step one (Hastad): we will use lattice reduction to find $F'(z)$ such that (a) the roots of $F \bmod N$ are also roots of $F' \bmod N$, and (b) F' has small coefficients. (We will use the variant due to Howgrave-Graham.)

* For polynomial $F(z) = \sum_{i=0}^{d} f_i z^i$ and bound X, denote

$$b_{F,X} = \langle f_0 \;\; f_1 X \;\cdots\; f_d X^d \rangle \in \mathbb{Z}^{d+1}$$

<u>Theorem</u>: For a polynomial $F(z)=\sum_{i=0}^{d} f_i z^i$, modulus M and bound $X<M$, if $\|b_{M,X}\| < \frac{M}{2\sqrt{d+1}}$ then every root z of $\underbrace{F}_{\text{mod } M}$ of size $|z|<X$ is also a root over the integers.

<u>Proof</u>: $|F(z)| \le \sum_{i=0}^{d} |f_i|\cdot|z^i| \le \sum_{i=0}^{d} |f_i|\cdot X^i \overset{(*)}{\le} \sqrt{d+1}\,\|b_{F,X}\| < M/2$, where inequality $(*)$ follows from Cauchy-Schwartz, $\left(\sum_{i=0}^{d} 1\cdot a_i\right)^2 \le \left(\sum_{i=0}^{d} 1^2\right)\left(\sum_{i=0}^{d} a_i^2\right)$ ⊠

* Assume that F is monic ($f_d=1$), and consider the lattice spanned by the columns of

$$B = \begin{pmatrix} M & & & & f_0 \\ & MX & & 0 & f_1 X \\ & & \ddots & & \vdots \\ & 0 & & MX^{d-1} & f_{d-1}X^{d-1} \\ & & & & X^d \end{pmatrix}, \quad \det(B)=M^d\cdot X^{d(d+1)/2}$$

Note that for every column of B, if we think of it as a vector $b_{G,X}$ for some polynomial G then for that polynomial G it holds that $G(z)=0 \bmod M$ for every root of F mod M. Hence the same holds for every vector in $\Lambda(B)$.

- Applying LLL to B, we can find a vector $V\in\Lambda(B)$ of size at most $\|V\| \le 2^{d/2}\cdot\sqrt{d+1}\cdot\det(B)^{1/d+1} = (2X)^{d/2}\cdot\sqrt{d+1}\cdot M^{d/d+1}$ ← the point is that this is less than M
- If $\|V\|$ is less than $\frac{M}{2\sqrt{d+1}}$ then every root of the corresponding $\underbrace{\text{polynomial}}_{\text{mod } M}$ which is smaller than X is also a root over the integers.
- So we can find all these small roots, and they are also roots of F mod M.
- We need $(2X)^{d/2}\cdot\sqrt{d+1}\cdot M^{d/d+1} < \frac{M}{2\sqrt{d+1}}$

$$\iff (2X)^{d/2}\cdot(2d+2) < M^{\frac{1}{d+1}}$$

$$\iff X < \frac{1}{2}(2d+2)^{-2/d}\cdot M^{2/d(d+1)}$$

For the example application we have $d=3$ and $M\sim 2^k$ so we can solve as long as our bound in

$$X=2^n < \frac{1}{2}\cdot 8^{-2/3}\cdot 2^{\frac{2k}{12}}$$

$$= 2^{k/6-3}$$

e.g. for RSA-1024 we can break when $n\le 167$

* Step 2 (Coppersmith): Can we do better than $X \le M^{\Theta(1/d^2)}$?

The idea: If $F(z) = 0 \bmod M$ then also $z \cdot F(z) = 0 \pmod{M}$, $F(z)^2 = 0 \pmod{M^2}$, and in general $z^i F(z)^j = 0 \pmod{M^j}$.

* Let's see what we get if we add the relations $z^i F(X) = 0$ for $i = 0, 1, \ldots, d-1$. We have the following matrix

$$
B = \underbrace{\begin{pmatrix}
M & & & & f_0 & 0 & \cdots & 0 \\
& MX & & 0 & f_1 X & f_0 X & \cdots & 0 \\
& & \ddots & & \vdots & \vdots & & \\
& & & MX^{d-1} & f_{d-1} X^{d-1} & f_{d-2} X^{d-1} & \cdots & f_0 X^{d-1} \\
& & & & X^d & f_{d-1} X^d & & f_1 X^d \\
& & & & & X^{d+1} & & f_2 X^{d+1} \\
& & 0 & & & & \ddots & \vdots \\
& & & & & & & X^{2d-1}
\end{pmatrix}}_{2d \times 2d}
$$

Now we have $\det(B) = M^d \cdot X^{d(2d-1)}$, hence LLL will give a vector of size $\|V\| \le 2^d \cdot \sqrt{2d} \cdot M^{1/2} \cdot X^{d-1/2}$ (note, power of M bounded away from 1)

Now to get $\|V\| < \frac{M}{2 \cdot \sqrt{2d}}$ it is enough to have

$$2^d \sqrt{2d}\, M^{1/2} X^{\frac{2d-1}{2}} < \frac{M}{2 \cdot \sqrt{2d}}$$

$$\iff (2X)^{\frac{2d-1}{2}} < M^{1/2} / 2^{5/2} \cdot d$$

$$\iff X < \frac{1}{2} M^{\frac{1}{2d-1}} \cdot \left(2^{5/2} \cdot d\right)^{-2/2d+1} \approx \frac{1}{2} M^{\frac{1}{2d-1}}$$

* Adding relations $F(z)^j = 0 \bmod M^j$ helps even more, since the condition on $\|V\|$ becomes $\|V\| \leq M^j / 2\sqrt{\text{degree}}$

Consider a quadratic polynomial $F(z) = z^2 + az + b$, so $F(z)^2 = z^4 + 2az^3 + (a^2+2b)z^2 + 2abz + b^2$, and consider the following lattice basis

$$B = \begin{pmatrix} M^2 & 0 & Mb & 0 & b^2 \\ & M^2X & MaX & MbX & 2abX \\ & & MX^2 & MaX^2 & (a^2+2b)X^2 \\ & & & MX^3 & 2aX^3 \\ & & & & X^4 \end{pmatrix}$$

$F(z)^2 = 0 \pmod{M^2}$

$MzF(z) = 0 \pmod{M^2}$

$MF(z) = 0 \pmod{M^2}$

We have $\det(B) = M^6 X^{10}$

So LLL can find a vector of size $\|V\| \leq 2^{\frac{5-1}{2}} \cdot \sqrt{5} \cdot M^{6/5} \cdot X^2$.

To use the theorem we need

$$\|V\| \leq \frac{M^2}{2\sqrt{5}}$$

$$\Leftarrow \quad 2^2 \cdot \sqrt{5} \cdot M^{6/5} \cdot X^2 < \frac{M^2}{2\sqrt{5}}$$

$$\Longleftrightarrow \quad X^2 < M^{4/5} / 80$$

$$\Leftarrow \quad X < M^{2/5} / 9$$

Note that if we use the relation $M z^2 F(z) = 0 \pmod{M^2}$ instead of $F(z)^2 = 0 \pmod{M^2}$ then the determinant will be larger (by a factor of M), and as a result we could only handle smaller bound $X < M^{3/10} / 9$

<u>Coppersmith's Theorem:</u> There exists poly-time algorithm that finds all the roots of $F(z) = 0 \pmod{M}$ whose size is at most M^δ, as long as $\delta \leq \frac{1}{\deg(F)} - \varepsilon$ (for any constant $\varepsilon > 0$).