The art of cryptography, summer 2013

Lattices and cryptography

Prof. Dr. Joachim von zur Gathen
Dr. Daniel Loebenberger

We use lattice basis reduction to find “small” roots of polynomials. The method will be applied to the cryptanalysis of RSA under special circumstances.

In order to recover an RSA plaintext from public and transmitted data, one has to compute x with $x^e = y$ in $\mathbb{Z}_N$, given only N, e, and y. In other words, she has to find a root modulo N of the polynomial $f = t^e - y \in \mathbb{Z}_N[t]$, where t is a variable.

For $u = (u_0, \ldots, u_{n-1}) \in \mathbb{R}^n$, we have the 1-norm of u

$$\|u\|_1 = \sum_{1 \leq i < n} |u_i|. \tag{1}$$

A famous result relating it to the 2-norm $\| \cdot \|$ is the Cauchy inequality:

$$\|u\|_1 \leq n^{1/2} \cdot \|u\|. \tag{2}$$

In the following, we identify a polynomial

$$g = \sum_{0 \leq i < n} g_i t^i \in \mathbb{Z}[t] \tag{3}$$

with its coefficient vector $(g_0, \ldots, g_{n-1}) \in \mathbb{Z}^n$. Thus

$$\|g\|_1 = \sum_{0 \leq i < n} |g_i|, \|g\| = (\sum_{0 \leq i < n} g_i^2)^{1/2}.$$

For any integers w and M we have

$$w = 0 \text{ in } \mathbb{Z}_M \text{ and } |w| < M \Longrightarrow w = 0. \tag{4}$$

LEMMA 5. *Let* $g \in \mathbb{Z}[t]$ *have degree less than* n, *let* c *and* M *be positive integers with*

$$n^{1/2} \cdot \|g(c \cdot t)\| < M,$$

and let $r \in \mathbb{Z}$ *satisfy* $|r| \leq c$ *and* $g(r) = 0$ *in* $\mathbb{Z}_M$. *Then* $g(r) = 0$ *in* $\mathbb{Z}$.

We choose some positive integer k. For $0 \leq j \leq k$, we have $N^{k-j} f(r)^j = 0$ in $\mathbb{Z}_{N^k}$, and we now want to take for g a linear combination of these $N^{k-j} f^j$. So we let

$$h_{ij} = N^{k-j} f^j t^i \in \mathbb{Z}[t]$$

for integers i and j with $0 \leq i < e = \deg f$ and $0 \leq j \leq k$. Then

$$h_{ij}(r) = 0 \text{ in } \mathbb{Z}_{N^k}$$

for all i, j. What we have gained is the much larger bound N^k instead of just N on $\|g(c \cdot t)\|$ that we can allow for M in Lemma 5. We then use basis reduction to compute an integral linear combination g of the $h_{ij}(c \cdot t)$.

ALGORITHM 6. Small polynomial with high-order roots.

Input: A monic linear polynomial $f \in \mathbb{Z}[t]$, positive integers N, c, and k, and real μ with $0 < \mu \leq 1$.
Output: $g \in \mathbb{Z}[t]$.

1. $n \longleftarrow \lceil k/\mu \rceil$.
2. $h_i \longleftarrow \begin{cases} N^{k-i} f^i & \text{for } 0 \leq i \leq k, \\ t^{i-k} f^k & \text{for } k < i < n. \end{cases}$
3. Form the $n \times n$ matrix A whose rows are the coefficient vectors of $h_0(ct), \ldots, h_{n-1}(ct)$.
4. Apply the basis reduction algorithm **??** to the rows of A, with output $B = UA$ and $U \in \mathbb{Z}^{n \times n}$ unimodular. Let $(u_0, \ldots, u_{n-1}) \in \mathbb{Z}^n$ be the top row of U.
5. Return $g = \sum_{0 \leq i < n} u_i h_i$.

Example 7. We trace the algorithm on the inputs $f = t + 53$, $N = 2183$, $c = 6$, $k = 4$, and $\mu = 1/2$. In step Algorithm 6 step 1, we have $n = 8$. The polynomials h_i are

$$h_0 = 22709885409121,$$
$$h_1 = 10403062487\,t + 551362311811,$$
$$h_2 = 4765489\,t^2 + 505141834\,t + 13386258601,$$
$$h_3 = 2183\,t^3 + 347097\,t^2 + 18396141\,t + 324998491,$$
$$h_4 = t^4 + 212\,t^3 + 16854\,t^2 + 595508\,t + 7890481,$$
$$h_5 = t^5 + 212\,t^4 + 16854\,t^3 + 595508\,t^2 + 7890481\,t,$$
$$h_6 = t^6 + 212\,t^5 + 16854\,t^4 + 595508\,t^3 + 7890481\,t^2,$$
$$h_7 = t^7 + 212\,t^6 + 16854\,t^5 + 595508\ t^4 + 7890481\,t^3.$$

Example (cont.). The 8×8 matrix A has as its rows the coefficients at $t^0, t^1, t^2, \ldots, t^7$ of $h_i(6t)$ and looks as follows:

22709885409121	0	0	0	0	0	0	0
551362311811	62418374922	0	0	0	0	0	0
13386258601	3030851004	171557604	0	0	0	0	0
324998491	110376846	12495492	471528	0	0	0	0
7890481	3573048	606744	45792	1296	0	0	0
0	47342886	21438288	3640464	274752	7776	0	0
0	0	284057316	128629728	21842784	1648512	46656	0
0	0	0	1704343896	771778368	131056704	9891072	279936

Step Algorithm 6 step 4 returns B and U, and the first rows of B and U are

$$b_0 = (-2163672, -4246020, 3044412, 315792, -970704, 1127520, 2612736, 279936),$$
$$u = (0, 2, -500, 52065, -1435989, 16363, -156, 1),$$

respectively.
The algorithm's output then is

$$\begin{aligned} g &= t^7 + 56t^6 + 145t^5 - 749t^4 + 1462t^3 + 84567t^2 - 707670t - 2163672 \\ &= (t-6) \cdot (t+53) \cdot (t^2 + 13t + 63) \cdot (t^3 - 4t^2 + 29t + 108). \end{aligned}$$

LEMMA 8. *The output of Algorithm 6 satisfies* $\deg g < n$ *and*

$$\|g(ct)\| \leq 2^{(n-1)/4} N^{k(k+1)/2\ell} c^{(n-1)/2}.$$

For any $r \in \mathbb{Z}$ *and a divisor* m *of* N, *we have*

$$f(r) = 0 \text{ in } \mathbb{Z}_m \Longrightarrow g(r) = 0 \text{ in } \mathbb{Z}_{m^k}.$$

The algorithm uses time polynomial in $\log(N \cdot \|f\|)$ *and* k/μ.

THEOREM 9. *Let f, N, c, k, and μ be an input for Algorithm 6, g the output, and*

$$\delta \geq \frac{1}{2} \log_N\left(\left(\frac{k}{\mu} + 1\right)2^{k/2\mu}\right), \quad (10)$$

$$c \leq N^{\mu^2 - \mu(\mu+2\delta)/k}, \quad (11)$$

and $m \geq N^\mu$ be a divisor of N. Then the set R of all integer roots of g has at most $\lceil k/\mu \rceil$ elements and contains all $r \in \mathbb{Z}$ with $f(r) = 0$ in $\mathbb{Z}_m$ and $|r| \leq c$. R can be computed in polynomial time.