The art of cryptography, summer 2013

Lattices and cryptography

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

computer Cosec b-it security

The hidden number problem

We have a prime p, and want to find an unknown integer s, given some high-order bits of st_i in $\mathbb{Z}_p$ for various random t_i.

More precisely: We are given $t_1, \ldots, t_n \in \mathbb{Z}_p^\times$, a positive integer α, and some $u_i \in V_\alpha(st_i \operatorname{srem} p)$ for each $i \leq n$, and want to compute $s \in R_p$.

We consider the lattice L spanned by the rows $a_0, \ldots, a_n$ of the following $(n+1) \times (n+1)$ matrix:

$$A = \begin{pmatrix} 1/\alpha & t_1 & t_2 & \cdots & t_n \\ 0 & p & 0 & \ldots & 0 \\ 0 & 0 & p & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p \end{pmatrix} \tag{1}$$

Algorithm 2. Finding a hidden number.

Input: A prime p, positive integers α and n, and $t = (t_1, \ldots, t_n) \in (\mathbb{Z}_p^\times)^n$ and $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$, so that there exists an (unknown) $s \in \mathbb{Z}_p$ with $u_i \in V_\alpha(t_i s \operatorname{srem} p)$ for all $i \leq n$.

Output: $s^* \in R_p$ with

$$u_i \in V_\alpha(t_i s^* \operatorname{srem} p) \text{ for all } i \leq n, \tag{3}$$

or "failure".

1. Run the basis reduction Algorithm 6 on the basis A in (1) and return a reduced basis B.
2. Let L be the lattice generated by B. Call the nearest hyperplane Algorithm 7 to return some $x = (x_0, \ldots, x_n) \in L$ which is $2^{(n+1)/2}$-close to u.
3. $s^* \longleftarrow x_0 \cdot \alpha$.
4. If (3) holds, then return s^* else return "failure".

THEOREM 4. *Let $p \geq 2^{36}$ be prime, $\lambda = (\log_2 p)^{1/2}$, $\epsilon = \lambda^{-1}$, $\alpha \geq 2^{5\lambda}$, $n = \lfloor \lambda/2 \rfloor$, and assume $s \in \mathbb{Z}_p$ as specified. There exists a set $E \subset (\mathbb{Z}_p^\times)^n$ with $\#E \leq p^{n(1-\epsilon)}$ such that for all inputs with $t \in (\mathbb{Z}_p^\times)^n \setminus E$, Algorithm 2 correctly computes s. The algorithm runs in polynomial time.*

COROLLARY 5. *Let $p \geq 2^{36}$ be prime, $\lambda = (\log_2 p)^{1/2}$, $\alpha = \lceil 2^{5\lambda} \rceil$, and $n = \lfloor \lambda/2 \rfloor$. If $t \xleftarrow{} (\mathbb{Z}_p^\times)^n$ is chosen randomly, then the success probability that $s^* = s$ of Algorithm 2 is at least*

$$1 - \frac{5^{\sqrt{\log_2 p}/2}}{\sqrt{p}} > 1 - 5 \cdot 10^{-4} > \frac{1}{2}.$$

ALGORITHM 6. Basis reduction.

Input: Linearly independent row vectors $a_1, \ldots, a_\ell \in \mathbb{Z}^n$.
Output: A reduced basis $b_1, \ldots, b_\ell$ of the lattice
$L = \sum_{1 \le i \le \ell} \mathbb{Z} a_i \subseteq \mathbb{Z}^n$.

1. For $i = 1, \ldots, \ell$ do $b_i \leftarrow a_i$.
2. Compute the GSO $B^* \in \mathbb{Q}^{\ell \times n}$, $M \in \mathbb{Q}^{\ell \times \ell}$,
3. $i \leftarrow 2$.
4. While $i \le \ell$ do 5–10
5. For $j = i-1, i-2, \ldots, 1$ do step
6. $b_i \leftarrow b_i - \lceil \mu_{ij} \rfloor b_j$, update the GSO, { replacement step }
7. If $i > 1$ and $\|b_{i-1}^*\|^2 > 2\|b_i^*\|^2$ then
8. exchange b_{i-1} and b_i and update the GSO, { exchange step }
9. $i \leftarrow i - 1$.
10. Else $i \leftarrow i + 1$.
11. Return $b_1, \ldots, b_\ell$.

ALGORITHM 7. Nearest hyperplane.

Input: A reduced basis $B = (b_1, \ldots, b_\ell)$ of an ℓ-dimensional lattice L in $\mathbb{R}^n$, and $u \in \mathsf{span}_{\mathbb{R}}(L) \subseteq \mathbb{R}^n$.
Output: $x \in L$ with $\|u - x\| \leq 2^{\ell/2} d(u, L)$.

1. Compute the GSO $(b_1^*, \ldots, b_\ell^*)$ of $(b_1, \ldots, b_\ell)$.
2. Compute $c = u \star b_\ell^* / (b_\ell^* \star b_\ell^*)$.
3. $c' \longleftarrow \lceil c \rfloor$,
   $v \longleftarrow u - (c - c')b_\ell^*$,
   $y \longleftarrow c' b_\ell$.
4. If $\ell = 1$, then return $x = y$. Else let M be the lattice generated by $b_1, \ldots, b_{\ell-1}$. Call the algorithm recursively to return $z \in M$ close to $v - y$.
5. Return $x = y + z$.