MASARYKOVA UNIVERZITA
Přírodovědecká fakulta
Název ústavu

Diplomová práce

Brno rok

Radim Čech

MASARYKOVA UNIVERZITA
Přírodovědecká fakulta
Název ústavu

Název práce na titulní list

Diplomová práce

Radim Čech

Vedoucí práce: Plné jméno včetně titulů **Brno rok**

Bibliografický záznam

Autor:	Plné jméno autora Přírodovědecká fakulta, Masarykova univerzita Název ústavu
Název práce:	Název práce
Studijní program:	Studijní program
Studijní obor:	Studijní obor
Vedoucí práce:	Plné jméno včetně titulů
Akademický rok:	rok/rok
Počet stran:	?? + ??
Klíčová slova:	Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo

Bibliographic Entry

Author:	Plné jméno autora Faculty of Science, Masaryk University Department of …
Title of Thesis:	Title of Thesis
Degree Programme:	Degree programme
Field of Study:	Field of Study
Supervisor:	Plné jméno včetně titulů
Academic Year:	rok/rok
Number of Pages:	?? + ??
Keywords:	Keyword; Keyword; Keyword; Keyword; Keyword; Keyword; Keyword; Keyword; Keyword

Abstrakt

V této bakalářské/diplomové/rigorózní práci se věnujeme ...

Abstract

In this thesis we study ...

Místo tohoto listu vložte kopii oficiálního zadání práce bez podpisů.

Poděkování

Na tomto místě bych chtěl(-a) poděkovat …

Prohlášení

Prohlašuji, že jsem svoji bakalářskou/diplomovou práci vypracoval(-a) samostatně pod vedením vedoucího práce s využitím informačních zdrojů, které jsou v práci citovány.

Prohlašuji, že jsem svoji rigorózní práci vypracoval(-a) samostatně s využitím informačních zdrojů, které jsou v práci citovány.

Brno xx. měsíce 20xx ....

Radim Čech

Obsah

Přehled použitého značení

Pro snažší orientaci v textu zde čtenáři předkládáme přehled základního značení, které se v celé práci vyskytuje.

$\mathbb{C}$	množina všech komplexních čísel

Úvod

Kapitola 1

Teorie

1.1 Lattice theory

Definition 1.1.1. Let B be a matrix with rows linearly independant rows $b_i \in \mathbb{R}^d$, then the discrete subgroup $\Lambda(B) = \{\sum v_i b_i | v_i \in \mathbb{Z}\}$ is called a *lattice*.

Let $\pi_i : \mathbb{R}^d \to \operatorname{span}(b_0, \ldots, b_{i-1})^\perp$ be the orthogonal projection into the complement. In particular, $\pi_0 \equiv id$. Then the *Gram-Schmidt orthogonalization* (GSO) of B is $B^* = (b_0, \ldots, b_{i-1})$, where $b_i^* = \pi_i(b_i) = b_i - \sum_{j=0}^{i-1} \mu_{i,j} \cdot b_j^*$ and $\mu_{i,j} = \langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle / \langle \boldsymbol{b}_j^*, \boldsymbol{b}_j^* \rangle$.

Let $||\cdot||$ be the euclidean norm. Denote by $\lambda_i(\Lambda)$ the radius of theh smallest ball centered at the origin containing at least i linearly independant lattice vectors. In particular, $\lambda_1(\Lambda)$ is the norm of the shortest vector of Λ.

Next we define the Gaussian heuristic to aproximate the shortest vector of a lattice.

Definition 1.1.2. Let $\Lambda(B)$ be a lattice. Denote by $\operatorname{vol}(\Lambda) = \det(B)$ the determinant of the basis and $\mathbb{B}_d(R)$ the d-dimensional euclidean ball. Then

$$\operatorname{gh}(\Lambda) = \left(\frac{\operatorname{Vol}(\Lambda)}{\operatorname{Vol}(\mathfrak{B}_d(1))} \right)^{1/d} = \frac{\Gamma\left(1 + \frac{d}{2}\right)^{1/d}}{\sqrt{\pi}} \cdot \operatorname{Vol}(\Lambda)^{1/d} \approx \sqrt{\frac{d}{2\pi e}} \cdot \operatorname{Vol}(\Lambda)^{1/d}$$

is called the *Gaussian heuristic*.

The main problem in lattice thoery is to find the shortest vector of a lattice.

Definition 1.1.3 (Shortest Vector Problem (SVP))**.** Let $\Lambda(B)$ be a lattice. Find the shortest nonzero vector in $\Lambda(B)$.

We will be interested in finding closest vector to the lattice which is guaranteed to not be too far away from the lattice.

Definition 1.1.4 (α-Bounded Distance Decoding (BDD$_\alpha$))**.** Given a lattice $\Lambda(B)$, a vector t and a parameter $\alpha > 0$ such that the euclidean distance between t and the lattice $\operatorname{dist}(t, B) < \alpha \cdot \lambda_1(\Lambda(B))$, find the lattice vector $v \in \Lambda(B)$ closest to t.

To guarantee a unique solution, it is required that $\alpha < 1/2$. There is a generalization of the problem for $1/2 < \alpha < 1$, where we want to find a unique solution with high probability. Asymptotically, for any polynomially-bounded $\gamma \geq 1$ there is a reduction from $\mathrm{BDD}_{1/\sqrt{2}\gamma}$ to $uSVP_\gamma$ from the following definition.

Definition 1.1.5 (γ-Unique Shortest Vector Problem(uSVP$_\gamma$))**.** Let Λ be a lattice such that $\lambda_2(\Lambda) > \gamma \cdot \lambda_1(\Lambda)$, find a nonzero vector $v \in \Lambda$ of length $\lambda_1(\Lambda)$.

The mentioned reduction is due to Kannan's embedding, that constructs

$$L = \begin{pmatrix} B & 0 \\ t & \tau \end{pmatrix}$$

where τ is some embedding factor. If v is the closest vector to t, then the lattice $\Lambda(L)$ contains $(t - v, \tau)$, which is small.

We will need some lattice algorithms.

Definition 1.1.6 (Enumeration)**.** Consider the following problem: Given a matrix B and a bound R, find all lattice vectors $v = \sum_{i=0}^{d-1} u_i \cdot b_i|_{u_i \in \mathbb{Z}}$ with some $u_i \neq 0$ and $\|v\|^2 < R^2$. Then by lattice vector enumeration we can pick the smallest one and solve the SVP.

We can rewrite the vector v with the Gram-Schmidt basis:

$$v = \sum_{i=0}^{d-1} u_i \cdot b_i = \sum_{i=0}^{d-1} u_i \cdot \left(b_i^* + \sum_{j=0}^{i-1} \mu_{i,j} \cdot b_j^* \right) = \sum_{j=0}^{d-1} \left(u_j + \sum_{i=j+1}^{d-1} u_i \cdot \mu_{i,j} \right) \cdot b_j^*.$$

And thanks to orthogonality, the norms of the projections $\pi_k(v)$ become

$$\|\pi_k(v)\|^2 = \left\| \sum_{j=k}^{d-1} \left(u_j + \sum_{i=j+1}^{d-1} u_i \, \mu_{i,j} \right) b_j^* \right\|^2 = \sum_{j=k}^{d-1} \left(u_j + \sum_{i=j+1}^{d-1} u_i \, \mu_{i,j} \right)^2 \cdot \|b_j^*\|^2.$$

So the norms play nicely with the parameter k. Begin with finding $\pi_d(v)$ such that $\|\pi_d(v)\|^2 < R^2$ and iterate the inequality over d. This defines a depth-first tree search. We find a candidate for u_{d-1} and continue to u_{d-2} level. Whenever we encounter no candidates, we abandon the branch and backtrack. When we reach the leaves u_0, we compare the candidates to the previously smallest found vector and backtrack.

Definition 1.1.7 (Sieving)**.** The lattice sieve algorithm takes a set of lattice vectors $L \subset \Lambda$ and searches for integer combinations that are short. By recursively doing this process we can solve the SVP.

Definition 1.1.8 (LLL)**.**

Definition 1.1.9 (BKZ)**.**

1.2 The Hidden Number Problem

Some leaks in the (EC)DCA and Diffie-Hellman can be mapped to the HNP, which is traditionally solved by lattice reduction or the Bleichenbacher attack.

Definition 1.2.1. Let q be prime, x a secret integer and $T_b = (q-1)/2^b$. An oracle generates random, uniformly distributed $c_j \in [1, \ldots, q-1]$, $k_j \in [-\lfloor T_{b+1} \rceil, \ldots, \lfloor T_{b+1} \rfloor]$ and computes

$$h_j = (k_j - c_j \cdot x) \mod q. \tag{1.1}$$

The adversery is given the pairs (h_j, c_j), $0 < j < L$ and the goal is to recover x. We call this an instance of the *hidden number problem* with a leak of b-bits.

In the (EC)DSA input, the nonces k are generally positive, but both the methods we will consider work for any sign of k. We can therefore reduce the bitsize by centering k around 0, i.e. substituting $\bar{k} = k - 2^{l-1}$. So that is the reason for the interval.

1.3 The Bleichenbacher Approach to the HNP

Definition 1.3.1. Let X be a random variable over $\mathbb{Z}\ q\mathbb{Z}$. Define *bias* of X as

$$B(X) = E(e^{2\pi i X/q}) = B(X \mod q). \tag{5}$$

For a set of points $V = (v_0, v_1, \ldots, v_{L-1})$ in $\mathbb{Z}/q\mathbb{Z}$, define the *sampled bias* as

$$B(V) = \frac{1}{L} \sum_{j=0}^{L-1} e^{2\pi i v_j/q}. \tag{6}$$

Lemma 1.3.2. *Let X be uniformly distributed on $[-(T-1)/2, \ldots, (T-1)/2]$ for some bound $0 < T \leq q$, then*

1. *For independent random variables X and Y, $B(X+Y) = B(X)B(Y)$.*
2. $B(X) = \frac{1}{T} \sin\left(\frac{\pi T/q}{\sin(\pi/q)}\right)$*. So $B(X)$ is real-valued and $0 \leq B(X) \leq 1$.*
3. *If $T = q$, then $B(X) = 0$.*
4. *Let a be an integer with $|a|T \leq q$, and $Y = aX$. Then $B(Y) = \frac{1}{T} \sin\left(\frac{\pi a T/q}{\sin(\pi a/q)}\right)$.*
5. $B(Y) \leq B(X)^{|a|}$.

Example 1.3.3 (Bias estimation)**.**

The idea of the Bleichenbacher attack is the following. Take a guess for the secret key $\omega \in \mathbb{Z}_q$ and let $B(\omega)$ be the bias of the set $\{h_j + c_j \cdot \omega \mod q\}$. Then we expect

$\omega = x$ to be the unique number such that the bias $B(\omega)$ will be significantly nonzero, while for all other $\omega \neq x$ the bias should be close to zero. To see this compute

$$\begin{aligned}
B_q(\omega) &= \frac{1}{L}\sum_{j=0}^{L-1} e^{2\pi i(h_j+c_j\omega)/q} = \sum_{t=0}^{q-1}\left(\frac{1}{L}\sum_{\{j|c_j=t\}} e^{2\pi i h_j/q}\right) e^{2\pi i t\omega/q} \\
&= \sum_{t=0}^{q-1}\left(\frac{1}{L}\sum_{\{j|c_j=t\}} e^{2\pi i(h_j+c_jx)/q}\right) e^{2\pi i t(\omega-x)/q} \\
&= \sum_{t=0}^{q-1}\left(\frac{1}{L}\sum_{\{j|c_j=t\}} e^{2\pi i k_j/q}\right) e^{2\pi i t(\omega-x)/q}. \qquad (1.2)
\end{aligned}$$

When $\omega = x$, $B(\omega) = \frac{1}{L}\sum_{j=0}^{L-1} e^{2\pi i k_j/q}$ is exactly the sampled bias of the k_js. Assuming a b-bit leak and L large enough, $B(X)$ will be close to 1, since the points $e^{2\pi i k_j/q}$ lie in the part of the unit circle with phase $-\pi/2^b < \theta < \pi/2^b$. $B(\omega)$ will be close to zero for $\omega \neq x$, since the points will be distributed over the whole circle because of the $e^{2\pi i t(\omega-x)/q}$ term in (1.2).

Now evaluating this sum for all $\omega \in \mathbb{Z}_q$ is not feasible. Notice from (1.2) that $B(\omega)$ is a sum of terms $e^{2\pi i t\omega/q}$ with frequencies t/q. If the frequencies t/q are much smaller than 1, then the peak of $B(\omega)$ will broaden allowing us to search only over a sparse set of ω. To achieve this we need to reduce the size of the c_js. Assuming that $c_j < C$ for some C, and letting $n = 2C$, we can find the n most significant bits of x by searching for a peak in n evenly spaced values of $\omega \in \mathbb{Z}_q$. Set $\omega_m = mq/n, m \in [0, n-1]$. Then

$$\begin{aligned}
B_q(\omega_m) &= \frac{1}{L}\sum_{j=0}^{L-1} e^{2\pi i(h_j+(c_jmq/n))/q} = \frac{1}{L}\sum_{j=0}^{L-1} e^{(2\pi i h_j/q)+(2\pi i c_j m/n)} \\
&= \sum_{t=0}^{n-1}\left(\frac{1}{L}\sum_{\{j|c_j=t\}} e^{2\pi i h_j/q}\right) e^{2\pi i t m/n} = \sum_{t=0}^{n-1} Z_t e^{2\pi i t m/n}. \qquad (8)
\end{aligned}$$

is the inverse FFT of $Z = (Z_0, \ldots, Z_{n-1})$. Find the m for which $B(\omega_m)$ is maximal, then the most significant n bits of x are $msb_n(x) = msb_n(mq/n)$. So n is determined by the maximum FFT we can compute. If we can reduce the c_j below C, then we can iteratively recover the whole secret key.

1.3.1 Range reduction

There are various approaches to range reduction. The original Bleichenbacher presentation proposes the sort and difference algorithm.

1. Sort the list $\{(h_i, s_i)\}_{i=0}^{L-1}$ in ascending order by the h_i values.

2. Take the successive differences to create a new list $\{(h'_i, s'_i)\}_{i=0}^{L-2} = \{(h_{i+1} - h_i, s_{i+1} - s_i)\}_{i=0}^{L-2}$.

3. Repeat.

In the original presentation, Bleichenbacher mentioned the use of the Schroeppel–Shamir algorithm, a knapsack problem solver, for the range reduction phase. The paper (newbleichenbahcer records) transforms the Schroeppel–Shamir knapsack solver into a range reduction algorithm. The idea is to

1. Split the set S of $2^{\alpha+2}$ of input signatures into 4 lists $\mathcal{L}^1, \mathcal{R}^1, \mathcal{L}^2, \mathcal{R}^2$ of size 2^α.
2. Fix a $c \in [0, 2^\alpha] \cap \mathbb{Z}$ and create lists $\mathcal{A}^r, r \in 1, 2$, that contain the combinations of two samples $(\eta^r, \xi^r) = \mathcal{L}^r(i) + \mathcal{R}^r(j) = (c_i^r + c_j^r, h_i^r + h_j^r)$ such that η^r's $(\alpha+1)$ most significant bits are the same as c's, that is $MSB_{\alpha+1}(\eta^r) = MSB_{\alpha+1}(c)$.
3. Sort $\mathcal{A}^1, \mathcal{A}^2$ by the first coordinate and extract short combinations.

pseudokod je v (new bleichanbcher)

1.4 Solving the HNP with Lattices

Papers related to the lattice approach define the leak simply as $k_j \in [-2^l, \dots, 2^l] \cap \mathbb{Z}$ for some l. Let q be an s-bit prime, then $q < 2^s$ and $(q-1)/2^b < 2^{s-b}$. So we can relax the bound and assume $k_j \in [-2^l, \dots, 2^l] \cap \mathbb{Z}$, for $l = s - b$.

Boneh and Vankatesan construct the following lattice for solving the HNP

$$\begin{bmatrix} n & 0 & 0 & \cdots & 0 & 0 \\ 0 & n & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n & 0 \\ c_0 & c_1 & c_2 & \cdots & c_{m-1} & \frac{1}{n} \end{bmatrix}, \tag{1.3}$$

and we want to find the vector $(h_0, \dots, h_{m-1}, 0)$. We have $(h_j + c_j \cdot x) \mod q = k_j$ and $|k_j| < 2^l$. Therefore the vector $([c_0 \cdot x]_p, \dots, [c_{m-1}x]_p, x/n)$ is within $\sqrt{m+1} \cdot 2^l$ of the desired vector for $|k_i| < 2^l$.

By the uniqueness theorem (boneh) if we can solve the CVP, we can solve the hidden number problem. We proceed by transforming the CVP to the SVP via Kannan's embedding. Construct the lattice

$$\begin{bmatrix} n & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & n & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n & 0 & 0 \\ c_0 & c_1 & c_2 & \cdots & c_{m-1} & 2^\ell/n & 0 \\ h_0 & h_1 & h_2 & \cdots & h_{m-1} & 0 & 2^\ell \end{bmatrix}$$

This lattice contains a vector

$$(k_0, k_1, \dots, k_{m-1}, 2^\ell \cdot x/n, 2^\ell),$$

which has norm at most $\sqrt{m+2} \cdot 2^l$. This lattice also contains $(0, \dots, 2^l, 0)$, so it is not generally the shortest vector. Heninger suggests some improvements for this lattice.

By eliminating x from the 0-th equation $h_0 = (k_j - c_j x) \mod q$ we get

$$-c_0^{-1}(h_0 - k_0) = x \mod q$$

Now by eliminating x from the j-th equation we get

$$h_j - c_j \cdot c_0^{-1} h_0 = (k_j - c_j \cdot c_0^{-1} k_0) \mod q$$

Thus we have reduced the dimension of the lattice by 1. The vector $(0, \dots, 2^l, 0)$ is no longer in the lattice and the new target $(k_1, \dots, k_{m-1}, k_0, 2^l)$ is expected to be the unique shortest vector. This transformation is analogous to the normal form for LWE

Kapitola 2

Experiment

Závěr

Příloha

Seznam použité literatury

[1] S. J. Monaquel a K. M. Schmidt, *On M-functions and operator theory for non-self-adjoint discrete Hamiltonian systems*, v „Special Issue: 65th birthday of Prof. Desmond Evans“, J.Comput. Appl. Math. **208** (2007), č. 1, 82–101.