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

TODO boneh-venkatesan cely clanek prednaska

lovacs nerovnost dukaz

bleichenbacher

screenshot rozvrhu

oba dva pristupy pochopit na ideove a implementacni urovni(napsat pseudokod do textu)

proof of concept reseni obema zpusoby naprogramovat

Sepsat LLL a dopsat odvozeni delta

1.1 Lattice theory

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 1.1.1. 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 1.1.2 (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 1.1.3 (α-Bounded Distance Decoding (BDD_α))**.** Given a lattice $\Lambda(B)$, a vector t and a parameter $\alpha > 0$ such that the euclidean distance between t and the lattice $\mathrm{dist}(t, B) < \alpha \cdot \lambda_1(\Lambda(B))$, 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 1.1.4 (γ-Unique Shortest Vector Problem(uSVP_γ))**.** 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 1.1.5 (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 1.1.6 (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 1.1.7 (BKZ)**.**

1.2 The Hidden Number Problem

Definition 1.2.1. Let n be prime, and α is a secret integer. An oracle generates random, uniformly distributed $t_i \in \mathbb{Z}_n$ and computes

$$s_i = t_i \cdot \alpha \mod n \tag{1.1}$$

and reveals some most important bits of s_i and t_i. The adversery is given the pair (t_i, a_i) with the revealed bits. Then we can write (1.1) as

$$a_i + k_i = t_i \cdot \alpha,$$

where $k_i < 2^l$ for some parameter $l \in \mathbb{N}$.

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.

1.2.1 Solving the HNP with Lattices

Boneh and Vankatesan construct the following lattice for solving the HNP

$$\begin{bmatrix} n & 0 & 0 & \cdots & 0 & 0 \\ 0 & n & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n & 0 \\ t_0 & t_1 & t_2 & \cdots & t_{m-1} & \frac{1}{n} \end{bmatrix}, \tag{1.2}$$

and we want to find the vector $(a_0, \ldots, a_{m-1}, 0)$. The vector $([t_0 \cdot \alpha]_p, \ldots, [t_{m-1}\alpha]_p, \alpha/n)$ is within $\sqrt{m+1} \cdot 2^l$ of the desired vector for $|k_i| < 2^l$.

1.2.2 HNP and Bleichenbacher

eHNP,

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.