國立臺灣大學電機資訊學院電機工程學系

碩(博)士論文

Department of Electrical Engineering

College of Electrical Engineering and Computer Science

National Taiwan University

Master Thesis / Doctoral Dissertation

論文名稱

English Title

你的名字

English Name

指導教授：他的名字 博士

Advisor: his English name, Ph.D.

中華民國 109 年 3 月 (6日)

March 6, 2020

誌謝

需要感謝的人太多了，就感謝天罷！
你的論文趕快寫完，就謝天謝地嘍！

Abstract

Content of abstract

Keywords: *Cryptography*

摘要

摘要內容

關鍵字: 臺大椰林、總圖。

Contents

List of Tables

List of Figures

List of Algorithms

Chapter 1

Introduction

This is an example of table. We recommend the online Latex Generator: https://www.tablesgenerator

Algorithm	Time Complexity	Space Complexity
AKS Sieve [AKS01]	$2^{3.346n+o(n)}$	$2^{2.173n+o(n)}$

Table 1.1: Example of table

1.1 Contributions and Roadmap

write it down or not.

- **Taiwan No. 1** Good

Figure 1.1: Just an example

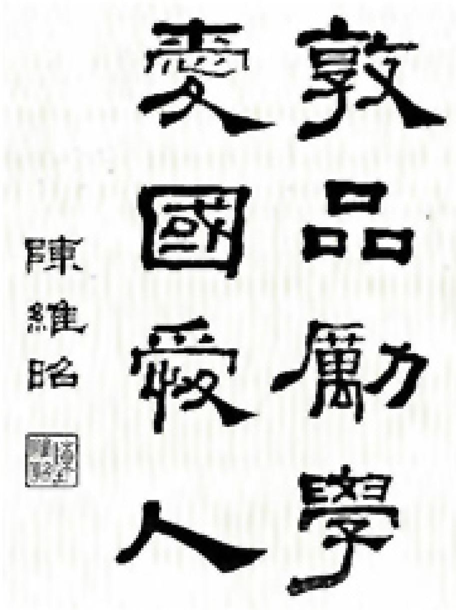

Figure 1.2: me too

Chapter 2

Preliminary

2.1 Definition and Notation

This is different

Examples

Problem Descriptions

Problem Property This is an example of equations.

$$\|\sum_{t=1}^{n} u_t \vec{b}_t\| = \min_{x\in\mathbb{Z}^n} \|\sum_{t=1}^{n} x_t \vec{b}_t\|$$

we replace all $\vec{b}_t$ by their orthogonalization, i.e., $\vec{b}_t = \vec{b}_t^* + \sum_{j=1}^{t-1} \mu_{t,j} \vec{b}_j^*$ and get a degree.

Algorithm 1 This is an example of algorithm.

Require: basis B($\vec{b}_1, ..., \vec{b}_n$), PrunedBound $R_1^2 \leq R_2^2 \leq ... \leq R_n^2$
Ensure: The coefficients $(x_1, ..., x_n)$ of the basis satisfying the Pruned Bound

Compute Gram-Schmidt orthogonalization μ of basis B
$\sigma \leftarrow (0)_{(n+1)\times n}$
while *true* **do**
  $\rho_k = \rho_{k+1} + (v_k - c_k)^2 \|b_k^*\|^2$
  if $\rho_k \leq R_{n+i-k}^2$ **then**
    if $k = 1$ **then**
      return $(v_1, ..., v_n)$
    else
      $k \leftarrow k - 1$
      $r_{k-1} \leftarrow max(r_{k-1}, r_k)$
      for $i = r_k$ downto $k + 1$ **do**
        $\sigma_{i,k} \leftarrow \sigma_{i+1,k} + v_k \mu_{i,k}$
      end for
      $c_k \leftarrow -\sigma_{k+1,k}$
      $v_k \leftarrow \lfloor c_k \rceil$; $w_k = 1$;
    end if
  else
    $k \leftarrow k + 1$
  end if
end while

Bibliography

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In Jeffrey Scott Vitter, Paul G. Spirakis, and Mihalis Yannakakis, editors, *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 601–610. ACM, 2001.

Appendices

Appendix A

Proof for example

A.1 title

Here we consider the case of $q = 12289$, $k = 3$. The input U, V satisfies the following condition.

$$V = V_0 + V_1 \cdot 2^{12} + V_2 \cdot 2^{24} \text{ and } U = U_0 + U_1 \cdot 2^{12}$$

$$\text{where } 0 \leq V_0 < 2^{12},\ 0 \leq V_1 < 2^{12},\ 0 \leq V_2 < 2^{6},\ 0 \leq U_0 < 2^{12}, \text{ and } 0 \leq U_1 < 2^{4}$$

$$A = \texttt{K-RED}(U) = 3U_0 - U_1 \text{ and } B = \texttt{K-RED2x}(V) = 9V_0 - 3V_1 + V_2$$