Title of the thesis

TITLE OF THE THESIS

BY

FIRST LAST[1], B.Eng.

A THESIS

SUBMITTED TO THE DEPARTMENT OF COMPUTING AND SOFTWARE

AND THE SCHOOL OF GRADUATE STUDIES

OF MCMASTER UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

Master of Applied Science (20xx)	McMaster University
(Software Engineering)	Hamilton, Ontario, Canada

TITLE:	Title of the thesis
AUTHOR:	First Last[3] B.Eng. (Software Engineering) McMaster University, Hamilton, Ontario, Canada
SUPERVISOR:	Dr. First Last
NUMBER OF PAGES:	xi, 132

To my family

Abstract

Motivation paragraph.

What is the problem paragraph.

The meat of the thesis goes here (how we solve the problem).

Conclusion: why is our solution of interest.

Acknowledgements

Acknowledge 1st.

Acknowledge 2nd.

Any awards / bursaries that made this possible.

Acknowledge very special.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this chapter, we introduce XYZ. In Section 1.1, we give an introduction to XYZ and explain its ever-growing importance in today's society. In Section 1.2, we introduce XYZ and indicate their use in computer systems. In Section 1.3, we provide a review of the literature and discuss some existing techniques for XYZ while indicating how the existing techniques are not sufficient to ABC. In Section 1.4, we give the motivation for a new technique to ABC. In Section 1.5, we state the problem subject of our work. In Section 1.6, we summarize our contributions. Finally, in Section 1.7, we give the structure of the remainder of the thesis.

1.1 General Context

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio. Sed eu convallis felis. Nullam eget libero metus. Ut sed leo a nibh tempor vestibulum. Mauris leo nibh, consequat sed vehicula ac, rhoncus sit amet ligula. Vestibulum efficitur ornare ullamcorper. In rhoncus mollis condimentum.

Lorem ipsum has three facets which have a strong relationship to ABC: confidentiality, integrity, and availability [Bis02]. Confidentiality refers to consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio. Integrity refers to consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio. Availability refers to the consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio. Confidentiality, integrity, and availability are strongly related to consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio.

1.2 Specific Context

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio. Sed eu convallis felis. Nullam eget libero metus. Ut sed leo a nibh tempor vestibulum. Mauris leo nibh, consequat sed vehicula ac, rhoncus sit amet ligula. Vestibulum efficitur ornare ullamcorper. In rhoncus mollis condimentum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet [Lam73]. Etiam ut nisi odio. Sed eu convallis felis. Nullam eget libero metus. Ut sed leo a nibh tempor vestibulum [Kem83]. Mauris leo nibh, consequat sed vehicula ac, rhoncus sit amet ligula. Vestibulum efficitur ornare ullamcorper. In rhoncus mollis condimentum.

1.3 Literature Survey of XYZs

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio [GM82]. Sed eu convallis felis. Nullam eget libero metus. Ut sed leo a nibh tempor vestibulum. Mauris leo nibh, consequat sed vehicula ac, rhoncus sit amet ligula. Vestibulum efficitur ornare ullamcorper. In rhoncus mollis condimentum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed posuere eros ac nisi feugiat commodo. Curabitur sit amet ex feugiat, efficitur felis ut, mollis massa. Aliquam odio quam, tincidunt ut efficitur nec, condimentum in odio. Duis sagittis in risus id laoreet. Etiam ut nisi odio. Sed eu convallis felis. Nullam eget libero metus. Ut sed leo a nibh tempor vestibulum. Mauris leo nibh, consequat sed vehicula ac, rhoncus sit amet ligula. Vestibulum efficitur ornare ullamcorper. In [NW06] rhoncus mollis condimentum.

1.4 Motivation

Sed sit amet elementum ligula. Vivamus faucibus, augue vel tincidunt elementum, sapien est ullamcorper nisl, non gravida urna massa a eros. Nulla sit amet feugiat leos [Gra00]. Pellentesque id ante consectetur purus imperdiet tincidunt a tincidunt diam. Mauris sagittis sollicitudin cursus. Morbi elementum arcu quis mollis gravida. Mauris id accumsan libero. Morbi scelerisque id nibh eget venenatis. Curabitur iaculis mi at urna varius malesuada. In luctus risus non justo hendrerit commodo.

Proin ultricies enim sit amet libero fermentum convallis. Nunc blandit mauris ante, non vulputate justo feugiat at. Sed a cursus eros. In condimentum massa leo, vel sollicitudin eros egestas nec. Donec in tincidunt ex, sit amet fermentum est. Maecenas maximus lacus auctor tellus fermentum, in dapibus quam efficitur. Nunc pellentesque suscipit purus, ac tempus urna. Praesent nec libero luctus, faucibus velit eget, malesuada turpis. In commodo porta odio at aliquam. Suspendisse molestie dui at lacus suscipit, in auctor augue ultrices. In euismod fermentum justo, eget rutrum ligula gravida porta. Nam eu rhoncus nulla. Sed faucibus enim libero, non venenatis leo pharetra nec. Mauris et eros quis quam condimentum vulputate. Pellentesque nisl diam, ultrices non facilisis lobortis, hendrerit vitae turpis.

1.5 Problem Statement

Etiam erat odio, tempor vel mi eu, porta pretium lacus. Fusce dictum faucibus porttitor. Nunc vulputate mauris sed odio aliquet volutpat. Integer lorem dolor, volutpat a sagittis vitae, efficitur at turpis. Phasellus sodales tortor ac nunc tincidunt lobortis. Mauris dictum auctor nibh, ut aliquam dolor feugiat eu. Nullam pellentesque urna sed mauris fringilla, vel ornare nunc ornare. Nullam ac sollicitudin arcu. Nullam a accumsan orci.

Etiam erat odio, tempor vel mi eu, porta pretium lacus. Fusce dictum faucibus porttitor. Nunc vulputate mauris sed odio aliquet volutpat. Integer lorem dolor, volutpat a sagittis vitae, efficitur at turpis. Phasellus sodales tortor ac nunc tincidunt lobortis. Mauris dictum auctor nibh, ut aliquam dolor feugiat eu. Nullam pellentesque urna sed mauris fringilla, vel ornare nunc ornare. Nullam ac sollicitudin arcu. Nullam a accumsan orci.

1.6 Main Contributions

The main contributions to the XYZ include:

(i) Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.

(ii) Curabitur rutrum non lacus id tristique. Duis efficitur condimentum risus ac egestas.

(iii) Mauris id dapibus quam, non mollis purus. Ut vel iaculis sem. Morbi erat urna, cursus nec vehicula et, finibus ut nisi. Aenean eget nulla dui.

1.7 Structure of the Thesis

The remainder of this thesis is organized as follows:

Chapter 2 introduces the required mathematical background including MNO theory.

Chapter 3 provides a number of examples of ways in which XYZ.

Chapter 4 describes the process by which we formulate a new technique to ABC.

Chapter 5 gives a number of illustrative examples demonstrating the application of the proposed XYZ.

Chapter 6 discusses the impact of our approach in helping to remedy the problem of XYZ.

Chapter 7 draws conclusions and suggests future work.

Chapter 2

Mathematical Background

In this chapter, we introduce the necessary mathematical concepts required for the understanding of the material presented in the thesis. In Section 2.1, we give an introduction to ABC. In Section 2.2, we give definitions and examples of EFG. Finally, in Section 2.3, we conclude with a summary of the core concepts and describe where they are used throughout the remainder of the thesis.

2.1 Section One

Donec scelerisque risus et sollicitudin consectetur. In ac mattis lorem. Quisque commodo odio dui, a iaculis metus tristique et. Suspendisse sit amet interdum nunc, pretium gravida metus. Suspendisse a erat egestas, egestas mi a, tincidunt mi. Vivamus justo orci, porttitor ac tincidunt sit amet, fringilla eget neque. Integer at cursus quam. Ut malesuada ullamcorper erat finibus vestibulum. Nulla ullamcorper, enim ac accumsan placerat, lorem magna consequat nulla, nec pulvinar lacus neque vel quam. Donec posuere velit in leo vestibulum bibendum. Sed scelerisque magna vel orci tempor, vel bibendum nulla consequat. Maecenas varius nec leo eget volutpat. Vivamus vulputate mollis blandit. Nulla ligula risus, tincidunt nec dolor ac, ornare ultricies risus [GS93].

Mauris fermentum, nibh mollis cursus congue, orci velit imperdiet libero, ac mollis nunc nunc ut ex. Etiam tellus nibh, pellentesque et turpis ac, aliquet maximus turpis. Etiam ornare justo ac sodales rutrum. Morbi sed tellus enim. Donec malesuada ante tortor, sit amet tempus turpis molestie venenatis. Sed vitae eros vitae elit ultricies tincidunt. Nullam quis velit semper nisi ullamcorper ullamcorper eu id elit. Cras malesuada vehicula purus, et mattis turpis volutpat eu.

2.2 Section Two

Donec scelerisque risus et sollicitudin consectetur. In ac mattis lorem. Quisque commodo odio dui, a iaculis metus tristique et. Suspendisse sit amet interdum nunc, pretium gravida metus. Suspendisse a erat egestas, egestas mi a, tincidunt mi. Vivamus justo orci, porttitor ac tincidunt sit amet, fringilla eget neque. Integer at cursus quam. Ut malesuada ullamcorper erat finibus vestibulum. Nulla ullamcorper, enim ac accumsan placerat, lorem magna consequat nulla, nec pulvinar lacus neque vel quam. Donec posuere velit in leo vestibulum bibendum. Sed scelerisque magna vel orci tempor, vel bibendum nulla consequat. Maecenas varius nec leo eget volutpat. Vivamus vulputate mollis blandit. Nulla ligula risus, tincidunt nec dolor ac, ornare ultricies risus [SS93].

Mauris fermentum, nibh mollis cursus congue, orci velit imperdiet libero, ac mollis nunc nunc ut ex. Etiam tellus nibh, pellentesque et turpis ac, aliquet maximus turpis. Etiam ornare justo ac sodales rutrum. Morbi sed tellus enim. Donec malesuada ante tortor, sit amet tempus turpis molestie venenatis. Sed vitae eros vitae elit ultricies tincidunt. Nullam quis velit semper nisi ullamcorper ullamcorper eu id elit. Cras malesuada vehicula purus, et mattis turpis volutpat eu.

Definition 2.2.1. *Given two sets, A and B, we define the Cartesian product $A \times B$ as*

$$A \times B = \{(x, y) \mid x \in A \ \wedge \ y \in B\}$$

2.3 Conclusion

The objective of this chapter is to give readers the required mathematical background of our approach. We have presented ABC and EFG since we will be ... will be discussed further in Chapter 4.

Chapter 3

Survey

In this chapter, we aim to provide some insight lorem ipsum dolor sit amet, consectetur adipiscing elit. In Section 3.1, I give a short discussion of the one. In Sections 3.2 and **??**, I present a non-exhaustive summary of ABC. In Section 3.3 we discuss how XYZ.

3.1 One

Lorem ipsum dolor sit amet [Ber07, BR05, GKT05, HZD05, PSCS07, PAK99, Sar06, ZAB07], consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

In consectetur eleifend blandit. Sed volutpat malesuada rutrum. Suspendisse vel lorem id dui finibus porta at sed massa. Integer aliquet felis sed dolor egestas, sit amet iaculis tellus laoreet. Aenean vitae convallis mauris, id gravida lacus. Integer dapibus pharetra euismod. Nullam risus arcu, placerat at iaculis sit amet, suscipit a leo. Maecenas sed mi in leo sollicitudin suscipit vitae vel dolor. Vestibulum massa nunc, bibendum non porta ac, laoreet bibendum purus. Etiam non ligula odio. Nam in eros a velit rhoncus sagittis. Integer dapibus enim nec dolor sagittis, eget tristique dolor tristique. In malesuada velit diam, in accumsan elit rhoncus nec. Aliquam rhoncus elit lectus, vel dictum tortor interdum ac. Cras leo sapien, ultricies eleifend bibendum a, efficitur in lorem. Mauris ac nibh euismod, venenatis odio at, molestie massa.

3.2 Two

In this section, I present a number of XYZ.

3.2.1 Two One

Lorem ipsum dolor sit amet [Com05], consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

In consectetur eleifend blandit. Sed volutpat malesuada rutrum. Suspendisse vel lorem id dui finibus porta at sed massa. Integer aliquet felis sed dolor egestas, sit amet iaculis tellus laoreet. Aenean vitae convallis mauris, id gravida lacus. Integer dapibus pharetra euismod. Nullam risus arcu, placerat at iaculis sit amet, suscipit a leo. Maecenas sed mi in leo sollicitudin suscipit vitae vel dolor. Vestibulum massa nunc, bibendum non porta ac, laoreet bibendum purus. Etiam non ligula odio. Nam in eros a velit rhoncus sagittis. Integer dapibus enim nec dolor sagittis, eget tristique dolor tristique. In malesuada velit diam, in accumsan elit rhoncus nec. Aliquam rhoncus elit lectus, vel dictum tortor interdum ac. Cras leo sapien, ultricies eleifend bibendum a, efficitur in lorem. Mauris ac nibh euismod, venenatis odio at, molestie massa.

Two one one

Lorem ipsum dolor sit amet [SK06], consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

Two one two

Lorem ipsum dolor sit amet [SK06], consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

3.2.2 Two two

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

Two two one

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl [Com05], non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

Two two two

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis finibus ipsum non maximus fermentum. Vivamus iaculis lobortis magna, sit amet blandit enim euismod quis. Morbi ultricies malesuada nisl Figure 3.1, non fermentum justo vulputate sit amet. Aliquam lorem justo, cursus in luctus in, blandit ut orci. Mauris maximus lectus aliquam erat tristique, at pulvinar nunc varius. In nulla mauris, hendrerit eget porta eu, gravida ac nulla. Ut eu facilisis justo.

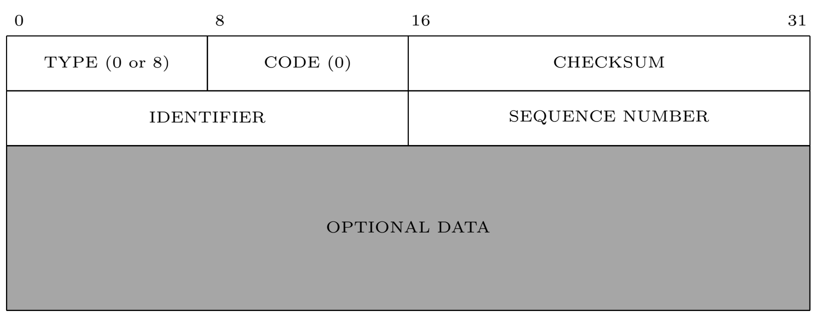


Figure 3.1: ICMP echo request or reply message format.

Pellentesque vitae imperdiet mi, vel semper arcu. Sed venenatis molestie elit, at malesuada sem suscipit non. In et tristique elit, sit amet aliquet arcu. Maecenas enim ex, aliquam nec diam vel, gravida tristique risus. Integer massa augue, porta sed dui quis, efficitur venenatis arcu.

3.2.3 Three

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras et nibh vel mauris pharetra viverra. Integer nisl nibh, ullamcorper eget imperdiet sed, accumsan ultrices purus. Quisque malesuada vel elit in cursus. Vestibulum rutrum turpis sed lectus vehicula, et venenatis ligula varius. Vivamus auctor fermentum libero, in ullamcorper diam pulvinar non. Donec condimentum cursus iaculis. Nulla odio dolor, faucibus eget mauris a, eleifend congue erat. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam aliquet finibus ligula eu feugiat. Aenean feugiat nunc et arcu elementum vestibulum.

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

3.3 Conclusion

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

Chapter 4

Main Chapter

In this chapter, we formulate a new XYZ. In Section 4.1, we list our assumptions. In Section 4.2, we give a clear mathematical representation of the problem of XYZ. In Section 4.3, we present our technique.

4.1 Assumptions

In formulating the problem of XYZ, we make the following assumptions:

(i) Assumption one.

(ii) Assumption two.

(iii) Assumption three.

4.2 Mathematical Representation

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras et nibh vel mauris pharetra viverra. Integer nisl nibh, ullamcorper eget imperdiet sed, accumsan ultrices purus. Quisque malesuada vel elit in cursus. Vestibulum rutrum turpis sed lectus vehicula, et venenatis ligula varius. In Section **??**, we discussed vivamus auctor fermentum libero, in ullamcorper diam pulvinar non. Donec condimentum cursus iaculis. Nulla odio dolor, faucibus eget mauris a, eleifend congue erat. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam aliquet finibus ligula eu feugiat. Aenean feugiat nunc et arcu elementum vestibulum.

Pellentesque aliquet tempor condimentum. Nulla vulputate ultricies felis, ut feugiat nisl auctor a. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas dapibus turpis ac tortor ullamcorper, in eleifend mi fringilla. Nam luctus tortor pulvinar neque molestie, quis scelerisque nisi volutpat. Integer et risus facilisis, vehicula libero nec, feugiat ante. In Figure 4.1, donec ultricies libero et mauris mollis, eu pretium neque iaculis. Sed in elit quis dui molestie dapibus vitae vel sapien. Etiam fermentum maximus accumsan.

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies.

$$\begin{tikzcd} & & \mathbb{D}_Q \\ \mathbb{N} \arrow[urr, "Q"] \arrow[rr, "P"'] & & \mathbb{D}_P \arrow[u, "X"'] \end{tikzcd}$$

Figure 4.1: Diagram representing the relationship between the relation P and Q via the abstraction relation X.

Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

4.3 The Proposed Technique

The proposed technique for the detection of the leak of confidential information via covert channels has two components: monitoring the information sent on the communication channels and finding an abstraction relation relating the confidential information to the information observed to be sent on the communication channel(s).

4.3.1 Monitoring the Communication Channels

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras et nibh vel mauris pharetra viverra. Integer nisl nibh, ullamcorper eget imperdiet sed, accumsan ultrices purus. Quisque malesuada vel elit in cursus. Vestibulum rutrum turpis sed lectus vehicula, et venenatis ligula varius. In Section **??**, we discussed vivamus auctor fermentum libero, in ullamcorper diam pulvinar non. Donec condimentum cursus iaculis. Nulla odio dolor, faucibus eget mauris a, eleifend congue erat. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam aliquet finibus ligula eu feugiat. Aenean feugiat nunc et arcu elementum vestibulum.

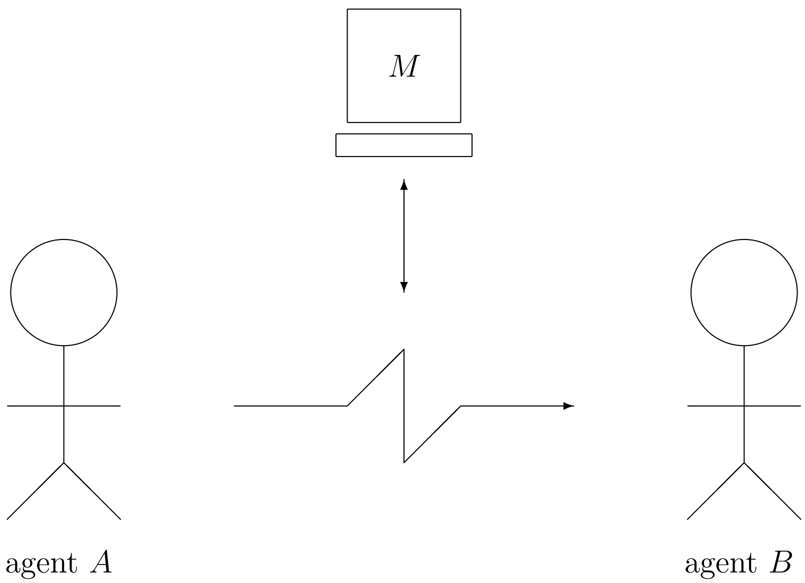


Figure 4.2: A scenario consisting of two agents communicating while being monitored.

Pellentesque aliquet tempor condimentum. Nulla vulputate ultricies felis, ut feugiat nisl auctor a. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas dapibus turpis ac tortor ullamcorper, in eleifend mi fringilla. Nam luctus tortor pulvinar neque molestie, quis scelerisque nisi volutpat. Integer et risus facilisis, vehicula libero nec, feugiat ante. Donec ultricies libero et mauris mollis, eu pretium neque iaculis. Sed in elit quis dui molestie dapibus vitae vel sapien. Etiam fermentum maximus accumsan.

4.4 Conclusion

Pellentesque aliquet tempor condimentum. Nulla vulputate ultricies felis, ut feugiat nisl auctor a. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas dapibus turpis ac tortor ullamcorper, in eleifend mi fringilla. Nam luctus tortor pulvinar neque molestie, quis scelerisque nisi volutpat. Integer et risus facilisis, vehicula libero nec, feugiat ante. Donec ultricies libero et mauris mollis, eu pretium neque iaculis. Sed in elit quis dui molestie dapibus vitae vel sapien. Etiam fermentum maximus accumsan

Chapter 5

Application of Main

In this chapter, we look at how the XYZ technique formulated in Chapter 4 can be applied to different scenarios involving ABC. Through a series of examples, we will see the versatility of the MNP technique and how it can be used to ABC.

In this chapter, we automate the given examples using the XYZ tool. For more information regarding the use of the XYZ tool, refer to Appendix A.

5.1 Application One

We continue with the illustrative example introduced in Section 4.3. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras et nibh vel mauris pharetra viverra. Integer nisl nibh, ullamcorper eget imperdiet sed, accumsan ultrices purus. Quisque malesuada vel elit in cursus. Vestibulum rutrum turpis sed lectus vehicula, et venenatis ligula varius. Vivamus auctor fermentum libero, in ullamcorper diam pulvinar non. Donec condimentum cursus iaculis. Nulla odio dolor, faucibus eget mauris a, eleifend congue erat. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam aliquet finibus ligula eu feugiat. Aenean feugiat nunc et arcu elementum vestibulum.

Through Example 5.1.1 we will show that nulla vulputate ultricies felis, ut feugiat nisl auctor a. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Example 5.1.1. *Consider a case where the set of confidential information is represented as* $P = \{(1,3),(2,1),(3,4),(4,1),(5,5),(6,9)\}$. *Suppose that agent A sends this information encrypted over a single communication channel as* $Q = \{(1,12),(2,1),(3,16),(4,1),(5,17),(6,18)\}$.

We define the relations P and Q in ***RELVIEW*** *as follows:*

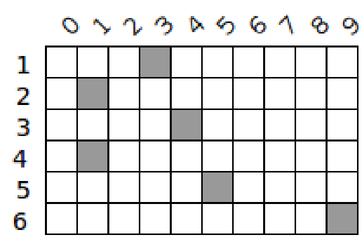


Figure 5.1: Relation P for Example 5.1.1.

We verify the existence of an abstraction relation by applying Corollary **??** *using* ***RELVIEW****. By executing Program A.2.1 (Result* $= Test(P,Q)$*), we obtain the following result:*

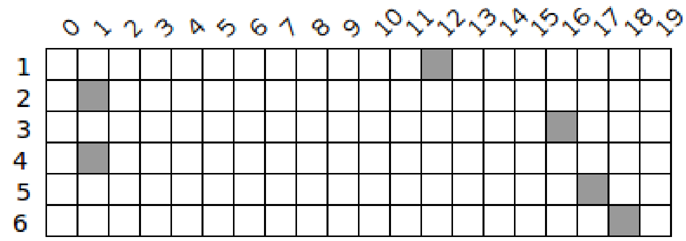


Figure 5.2: Relation Q for Example 5.1.1.

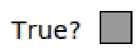


Figure 5.3: Relation *Result* for Example 5.1.1.

Therefore, the test has passed meaning that there exists an abstraction relation relating the confidential information to the information observed to be sent on the communication channel. This means that we can apply Corollary **??** *by executing Program A.2.2* ($X = Compute(P, Q, \mathbb{L})$) *to obtain the abstraction relation,* X*.*

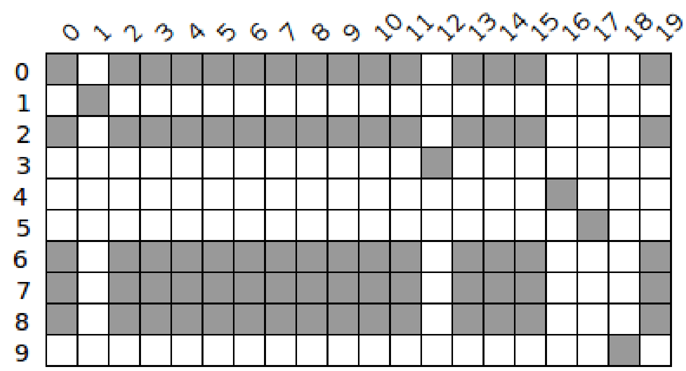


Figure 5.4: Abstraction relation X for Example 5.1.1.

From this result, we can see that there are some digits which are related to information which we do not necessarily have an interest in, i.e., we are only concerned with the confidential information which consists of the digits $1, 3, 4, 5,$ *and* 9*. Therefore* *we can design a filter R which can be used to refine the abstraction relation X. We define R in* ***RELVIEW*** *as follows:*

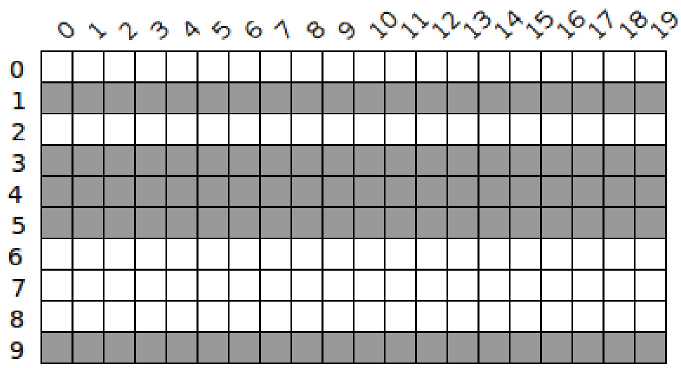


Figure 5.5: Filtering relation R for Example 5.1.1.

By executing Program A.2.2 with the filter R, ($X_{filtered} = Compute(P, Q, R)$), we obtain the abstraction relation, $X_{filtered}$

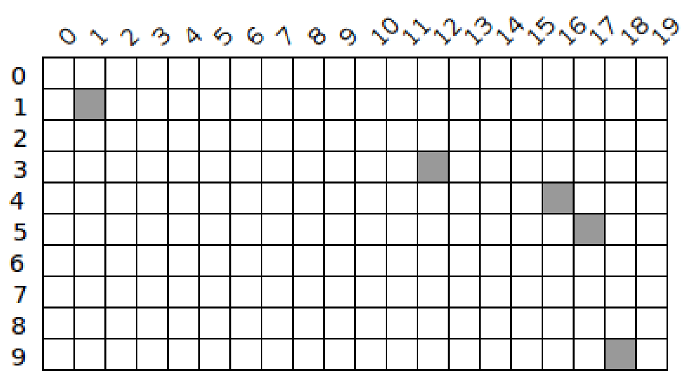


Figure 5.6: Abstraction relation $X_{filtered}$ for Example 5.1.1.

5.2 App Two

Pellentesque vitae imperdiet mi, vel semper arcu. Sed venenatis molestie elit, at malesuada sem suscipit non. In et tristique elit, sit amet aliquet arcu. Maecenas enim ex, aliquam nec diam vel, gravida tristique risus. Integer massa augue, porta sed dui quis, efficitur venenatis arcu. Sed massa dolor, auctor vitae felis eu, mollis mollis neque. Nunc luctus, sapien et auctor faucibus, justo metus ultricies nulla, nec consequat augue magna quis quam. Curabitur tristique bibendum vehicula. Sed quis dictum odio. Donec eget vestibulum sem. Nullam facilisis libero vel justo mattis luctus. Suspendisse auctor fringilla mi non varius. Proin vitae quam massa. Nam sit amet tristique urna, quis pharetra diam. Cras efficitur enim sed accumsan imperdiet. Vivamus euismod non odio nec semper.

Sed quis tellus maximus, condimentum mauris at, dictum diam. Curabitur faucibus, velit id vulputate facilisis, turpis quam molestie mi, ac imperdiet diam nisi ut tellus. Etiam ultrices orci at ante convallis, in rhoncus lacus posuere. Nam vel ullamcorper leo, eu aliquet ante. Cras venenatis sagittis mauris efficitur fringilla. Maecenas at pretium arcu. Duis rhoncus lorem metus, quis laoreet eros porttitor vitae.

This idea is best illustrated through Example 5.2.1.

Example 5.2.1. *Assume the set of confidential information is given as* $P = \{(1,3),(2,1),(3,4),(4,1),(5,5),(6,9)\}$. *In order to obscure the transmission of the information, agent A modulates the confidential information by a relation represented by*

$M = \{(0,9),(1,0),(2,1),(3,2),(4,3),(5,4),(6,5),(7,6),(8,7),(9,8)\}$ *prior to its encryption. Then, the new relation representing the confidential information is given by* $(P\,;M) = \{(1,2),(2,0),(3,3),(4,0),(5,4),(6,8)\}$. *This information is encrypted and sent on a single communication channel as* $Q = \{(1,11),(2,0),(3,12),(4,0),(5,16),(6,8)\}$.

*We define the relations P, M and Q in **`RELVIEW`** as follows:*

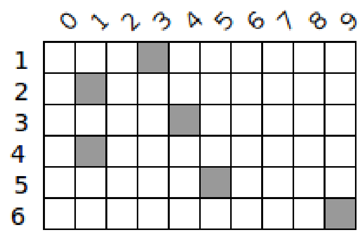


Figure 5.7: Relation P for Example 5.2.1.

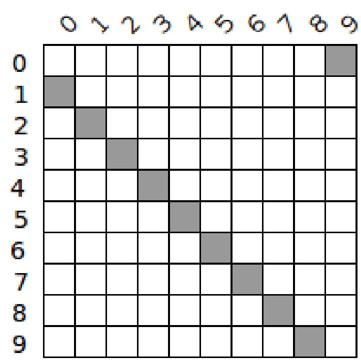


Figure 5.8: Modulation relation M for Example 5.2.1.

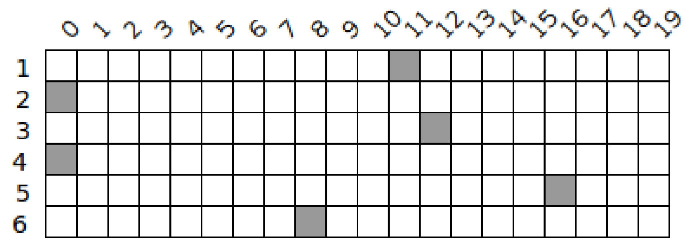


Figure 5.9: Relation Q for Example 5.2.1.

The modulated confidential information is represented in ***RELVIEW*** *as follows:*

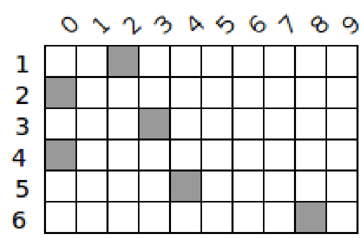


Figure 5.10: Relation $(P\,;M)$ for Example 5.2.1.

We verify the existence of an abstraction relation by executing Program A.2.1 (Result = $Test(P, Q)$*). In this case we are looking for an abstraction relation relating the confidential information, P, and the information sent on the communication channel, Q, which corresponds to the encrypted modulated confidential information.*

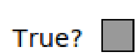


Figure 5.11: Relation *Result* for Example 5.2.1.

Therefore, the test has passed so we can compute the abstraction relation by executing Program A.2.2 ($X = Compute(P, Q, R)$) where R is the filtering relation.

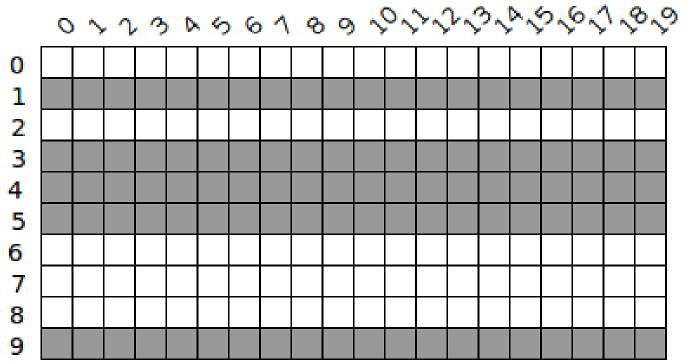


Figure 5.12: Filtering relation R for Example 5.2.1.

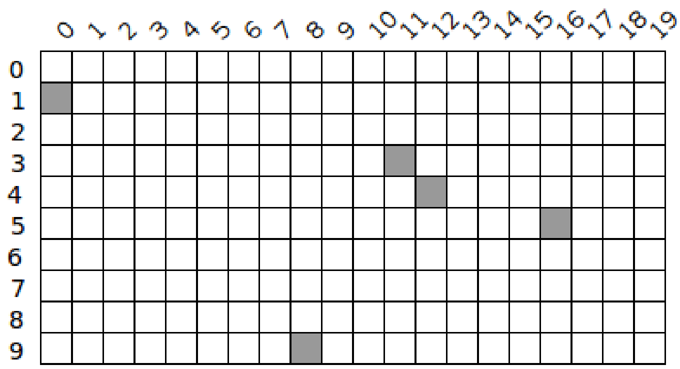


Figure 5.13: Abstraction relation X for Example 5.2.1.

5.3 Conclusion

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

Chapter 6

Discussion

In this chapter, we discuss various aspects of the problem ofXYZ. In Section 6.1, we discuss some possible application domains for which the XYZn technique presented in Chapter 4 is suitable. We also discuss the importance of such techniques and applications. In Section 6.2, we assess the strengths and weaknesses of the main contributions.

6.1 Discussion

Pellentesque aliquet tempor condimentum. The technique proposed in Chapter 4, nulla vulputate ultricies felis, ut feugiat nisl auctor a. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas dapibus turpis ac tortor ullamcorper, in eleifend mi fringilla. Nam luctus tortor pulvinar neque molestie, quis scelerisque nisi volutpat. Integer et risus facilisis, vehicula libero nec, feugiat ante. Donec ultricies libero et mauris mollis, eu pretium neque iaculis. Sed in elit quis dui molestie dapibus vitae vel sapien. Etiam fermentum maximus accumsan.

Pellentesque vitae imperdiet mi, vel semper arcu. Sed venenatis molestie elit, at malesuada sem suscipit non. In et tristique elit, sit amet aliquet arcu. Maecenas enim ex, aliquam nec diam vel, gravida tristique risus. Integer massa augue, porta sed dui quis, efficitur venenatis arcu. Sed massa dolor, auctor vitae felis eu, mollis mollis neque. Nunc luctus, sapien et auctor faucibus, justo metus ultricies nulla, nec consequat augue magna quis quam. Curabitur tristique bibendum vehicula. Sed quis dictum odio. Donec eget vestibulum sem. Nullam facilisis libero vel justo mattis luctus. Suspendisse auctor fringilla mi non varius. Proin vitae quam massa. Nam sit amet tristique urna, quis pharetra diam. Cras efficitur enim sed accumsan imperdiet. Vivamus euismod non odio nec semper.

6.2 Assessment of the Contributions

In this section, we discuss the strengths and weaknesses of the main contributions presented in this thesis. It is important to highlight both the strengths and weaknesses of the models and techniques that are developed so that we are able to further refine a solution to the problem of XYZ and possibly one day eliminate their use completely.

6.2.1 Strengths of the Contributions

Pellentesque vitae imperdiet mi, vel semper arcu. Sed venenatis molestie elit, at malesuada sem suscipit non. In et tristique elit, sit amet aliquet arcu. Maecenas enim ex, aliquam nec diam vel, gravida tristique risus. Integer massa augue, porta sed dui quis, efficitur venenatis arcu. Sed massa dolor, auctor vitae felis eu, mollis

mollis neque. Nunc luctus, sapien et auctor faucibus, justo metus ultricies nulla, nec consequat augue magna quis quam. Curabitur tristique bibendum vehicula. Sed quis dictum odio. Donec eget vestibulum sem. Nullam facilisis libero vel justo mattis luctus. Suspendisse auctor fringilla mi non varius. Proin vitae quam massa. Nam sit amet tristique urna, quis pharetra diam. Cras efficitur enim sed accumsan imperdiet. Vivamus euismod non odio nec semper.

Pellentesque vitae imperdiet mi, vel semper arcu. Sed venenatis molestie elit, at malesuada sem suscipit non. In et tristique elit, sit amet aliquet arcu. Maecenas enim ex, aliquam nec diam vel, gravida tristique risus. Integer massa augue, porta sed dui quis, efficitur venenatis arcu. Sed massa dolor, auctor vitae felis eu, mollis mollis neque. Nunc luctus, sapien et auctor faucibus, justo metus ultricies nulla, nec consequat augue magna quis quam. Curabitur tristique bibendum vehicula. Sed quis dictum odio. Donec eget vestibulum sem. Nullam facilisis libero vel justo mattis luctus. Suspendisse auctor fringilla mi non varius. Proin vitae quam massa. Nam sit amet tristique urna, quis pharetra diam. Cras efficitur enim sed accumsan imperdiet. Vivamus euismod non odio nec semper.

6.2.2 Weaknesses of the Contributions

Pellentesque vitae imperdiet mi, vel semper arcu. Sed venenatis molestie elit, at malesuada sem suscipit non. In et tristique elit, sit amet aliquet arcu. Maecenas enim ex, aliquam nec diam vel, gravida tristique risus. Integer massa augue, porta sed dui quis, efficitur venenatis arcu. Sed massa dolor, auctor vitae felis eu, mollis

mollis neque. Nunc luctus, sapien et auctor faucibus, justo metus ultricies nulla, nec consequat augue magna quis quam. Curabitur tristique bibendum vehicula. Sed quis dictum odio. Donec eget vestibulum sem. Nullam facilisis libero vel justo mattis luctus. Suspendisse auctor fringilla mi non varius. Proin vitae quam massa. Nam sit amet tristique urna, quis pharetra diam. Cras efficitur enim sed accumsan imperdiet. Vivamus euismod non odio nec semper.

6.3 Conclusion

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

Chapter 7

Conclusion and Future Work

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

7.1 Future Work

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

7.1.1 Theory: Models and Techniques

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

7.1.2 Applications

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

7.1.3 Tools/Automation

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

7.2 Closing Remarks

In imperdiet purus nec eleifend finibus. Aliquam non tempor massa. Etiam ac felis et ante varius vehicula nec eget tortor. Proin posuere quis felis non rutrum. Aenean quis felis ut ex sagittis pellentesque sit amet tempus nisl. Nam nec tellus ut lorem posuere semper non ac arcu. Nulla faucibus purus libero, in pellentesque sapien commodo tristique. Etiam consectetur lectus elit, id porttitor justo dignissim interdum. Donec ut nisl metus. Nulla sed dui lacus. Donec tristique dignissim massa sed ultricies. Maecenas iaculis arcu diam, ut dictum nisi euismod vitae. Praesent id imperdiet augue.

Appendix A

RELVIEW

To aid in the computation of the examples presented in this thesis, we use a tool called RELVIEW. RELVIEW is an interactive tool for computer-aided manipulation of relations represented as Boolean matrices. It is developed at the Department of Computer Science and Applied Mathematics at Christian-Albrechts-University in Kiel, Germany [Ber09]. This appendix presents an overview of working with RELVIEW and the programs developed in RELVIEW to automate the tests and computations of the corollaries presented in Chapter ??.

A.1 Working With RELVIEW

In this section, we look at how to work with relations using the RELVIEW tool. The information presented in this section is taken from [BBS09].

A.1.1 Representing Relations

`RELVIEW` is able to represent relations both as Boolean matrices and as an ASCII description.

Boolean Matrix Representation

The Boolean matrix representation of relations in `RELVIEW` is a graphical representation. A relation is given as a matrix where the rows represent the domain of the relation and the columns represent the range of the relation. A filled in cell of the matrix represents that element being included in the relation. An example of Boolean matrix representation of a relation in `RELVIEW` is given in Figure A.1.

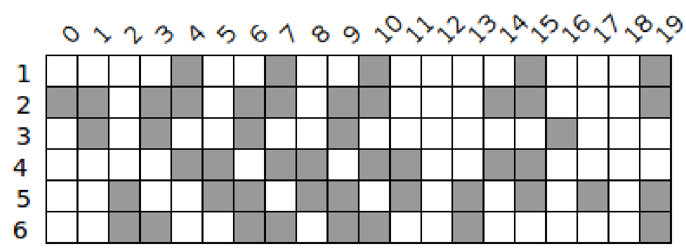


Figure A.1: Example of the Boolean matrix representation of a relation in `RELVIEW`.

ASCII Representation

The ASCII representation of relations in `RELVIEW` is a textual representation. A relation is given as a list entries of the form "`Domain : Range`". The ASCII representation of the relation given in Figure A.1 is given below.

```
R (6, 20)
1 : 5, 8, 11, 16, 20
2 : 1, 2, 4, 5, 7, 8, 10, 11, 15, 16, 20
3 : 2, 4, 7, 10, 17
4 : 5, 6, 8, 9, 11, 12, 15, 16
5 : 3, 6, 7, 9, 10, 12, 14, 16, 18, 20
6 : 3, 4, 7, 8, 10, 11, 14, 20
```

A.1.2 Operations

Syntax	Description
$-R$	Complement of relation R
$R \mid S$	Union (join) of R and S
$R \,\&\, S$	Intersection (meet) of R and S
$R + S$	Relational sum of R and S

Table A.1: Boolean Operations

Syntax	Description
$R\hat{}$	Converse of relation R
$R * S$	Composition of R and S

Table A.2: Relational Algebraic Operations

Syntax	Description
S/R	Left residue of R and S
$R\backslash S$	Right residue of R and S
$syq(R, S)$	Symmetric quotient of R and S

Table A.3: Residuals and Symmetric Quotients

Syntax	Description
$eq(R, S)$	Test, whether R and S are equal
$incl(R, S)$	Test, whether R is included in S

Table A.4: Relational Tests

A.1.3 Labels

Labels are organized into sets which are mappings from natural numbers to labels or identifiers.

The labels that are used in this thesis are given below:

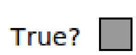
```
Digit = { 1 "0", 2 "1", 3 "2", 4 "3", 5 "4", 6 "5", 7 "6", 8 "7", 9
    "8", 10 "9" }

Encryption = { 1 "0", 2 "1", 3 "2", 4 "3", 5 "4", 6 "5", 7 "6", 8
    "7", 9 "8", 10 "9", 11 "10", 12 "11", 13 "12", 14 "13", 15 "14",
     16 "15", 17 "16", 18 "17", 19 "18", 20 "19" }

Bool = { 1 "True?" }
```

These labels are used in the Boolean matrix representation of relations making them easier to read and understand. The label “Digit” corresponds to the digit data type, the label “Encryption” corresponds to the natural numbers which can be used to encrypt the digits, and the label "Bool" simply adds a descriptive label for boolean results.

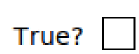
It is important to note that when representing relations using labels, the ASCII representation of the relation must correspond to the natural number and not the label or identifier. For example, if we want to represent the digit 4 being sent at time 1, i.e., $(1, 4)$ we must use "1 : 5" in the ASCII representation so that the label corresponds to the digit 4.

A.1.4 Truth Values

In `RELVIEW`, the result of a Boolean operation is a 1×1 Boolean matrix with the truth values corresponding to $\mathbb{L} = \mathsf{true}$ and $\emptyset = \mathsf{false}$. This is to say that the truth values are given by the Boolean matrices given in Figure A.2.



(a) True



(b) False

Figure A.2: `RELVIEW` representation of truth values.

A.2 `RELVIEW` Programs

Program A.2.1 represents the test outlined in Corollary ??.

Program A.2.1.

```
Test(p,q)
    DECL test1, test2, res
    BEG  test1 = eq(p,q*(q\p));
         test2 = eq(q,p*(p\q));
         res = test1 | test2
         RETURN res
    END.
```

Program A.2.2 corresponds to the computations presented in Corollary **??**.

Program A.2.2.

```
Compute(p, q, r)
    DECL test1, test2, res
    BEG  test1 = incl(p,q*(r^ & (q\p)));
         test2 = incl(q,p*(r  & (p\q)));
         IF test1 & test2
            THEN res = r & syq(p,q)
            ELSE IF test1
                THEN res = r & (q\p)^
                ELSE IF test2
                    THEN res = r & (p\q)
                    ELSE res = false
                FI
            FI
         FI
         RETURN res
    END.
```

Program A.2.3 automates the computation given in Corollary **??**.

Program A.2.3.

```
ComputeBij(p, q, r)
    DECL test1, test2, res
    BEG IF eq((p\q),(q\p)^)
            THEN res = r & (p\q)
            ELSE res = false
        FI
        RETURN res
    END.
```

Bibliography

[Ade10] S. Adee. Russian spies thwarted by old technology? IEEE Spectrum, June 29 2010.

[AR80] G.R. Andrews and R.P. Reitman. An axiomatic approach to information flow in programs. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 2(1):56 – 76, January 1980.

[BBS09] R. Behnke, R. Berghammer, and P. Schneider. Machine support of relational computations: The kiel relview system. Technical Report 9711, Christian-Albrechts-University of Kiel, 2009.

[Ber07] H. Berghel. Hiding data, forensics, and anti-forensics. *Communications of the ACM*, 50(4):15–20, April 2007.

[Ber09] Rudolf Berghammer. Relview. Available: `http://www.informatik.uni-kiel.de/~progsys/relview.shtml` (Accessed: July 27, 2010), July 2009.

[Bis02] Matt Bishop. *Computer Security: Art and Science*. Addison Wesley, Boston, MA, November 2002.

[BR05] R. Bidou and F. Raynal. Covert channels. November 2005.

[Bro94] R. Browne. Mode security: An infrastructure for covert channel suppression. In *Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 39 – 55, Los Almitos, CA, USA, 1994.

[Com05] D.E. Comer. *Internetworking with TCP/IP*, volume 1. Prentice Hall, fifth edition, 2005.

[Dao07] T. Dao. Analysis of the zodiac 340-cipher. Master's thesis, San Jose State University, December 2007.

[DoD85] United States of America Department of Defense. *Department of Defense Trusted Computer System Evaluation Criteria*. Number DoD 5200.28-STD in Defense Department Rainbow Series. Department of Defense / National Computer Security Center, Fort George G. Meade, Maryland, December 1985.

[FK98] H. Furusawa and W. Kahl. A study on symmetric quotients. Technical Report 1998-06, Fakultät für Informatik, Universität der Bundeswehr München, December 1998.

[GKT05] A. Grusho, A. Kniazev, and E. Timonina. Detection of illegal information flow. In *Proceedings of the Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Networked Security, MMM-ACNS 2005*, number 3685 in Lecture Notes in Computer Science, pages 235 – 244, Berlin, Germany, 2005.

[Gli93] V.D. Gligor. *A Guide to Understanding Covert Channel Analysis of*

Trusted Systems. Number NCSC-TG-030 in NSA/NCSC Rainbow Series. National Security Agency / National Computer Security Center, Fort George G. Meade, Maryland, November 1993.

[GM82] J.A. Goguen and J. Meseguer. Security policies and security models. In *Proceedings of the 1982 Symposium on Security and Privacy*, pages 11 – 20, New York, NY, USA, 1982.

[Gra00] J. W. Gray. Countermeasures and tradeoffs for a class of covert timing channels. Technical Report HKUST-CS94-18, Hong Kong University of Science and Technology, 2000.

[GS93] D. Gries and F.B. Schenider. *A Logical Approach to Discrete Math*. Springer Texts And Monographs In Computer Science. Springer-Verlag, New York, 1993.

[HH86a] C.A.R. Hoare and J. He. The weakest prespecification, part i. *Fundamenta Informaticae*, 1986.

[HH86b] C.A.R. Hoare and J. He. The weakest prespecification, part ii. *Fundamenta Informaticae*, 1986.

[Hoa69] C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576 – 580, October 1969.

[HZD05] L. Hélouët, M. Zeitoun, and A. Degorre. Scenarios and covert channels: Another game... *Electronic Notes in Theoretical Computer Science*, 119:93 – 116, 2005.

[HZJ03] L. Hélouët, M. Zeitoun, and C. Jard. Covert channels detection in protocols using scenarios. In *Proceedings of Security Protocols Verification, SPV'03*, pages 21 – 25, 2003.

[Jac90] J. Jacob. Separability and the detection of hidden channels. *Information Processing Letters*, 34(1):27 – 29, February 1990.

[JK01] R. Janicki and R. Khedri. On a formal semantics of tabular expressions. *Science of Computer Programming*, 39:189 – 213, March 2001.

[Kem83] R.A. Kemmerer. Shared resource matrix methodology: An approach to identifying storage and timing channels. *ACM Transactions on Computer Systems*, 1(3):256 – 77, August 1983.

[Khe98] R. Khedri. *Concurrence, Bisimulation et Équation d'Interface: Une Approche Relationnelle*. PhD thesis, Université Laval, April 1998.

[KM93] M.H. Kang and I.S. Moskowitz. A pump for rapid, reliable, secure communication. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 119 – 129, Fairfax, VA, USA, 1993.

[KP91] R.A. Kemmerer and P.A. Porras. Covert flow trees: A visual approach to analyzing covert storage channels. *IEEE Transactions on Software Engineering*, 17(11):1166 – 1185, November 1991.

[Lam73] B.W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613 – 615, October 1973.

[LMST+04] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina, and E. Tronci. Automatic covert channel analysis of a multilevel secure component. In

Proceedings of the 6th International Conference, ICICS 2004, number 3269 in Lecture Notes in Computer Science, pages 249 – 261, Berlin, Germany, 2004.

[Low02] G. Lowe. Quantifying information flow. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop, CSFW-15*, pages 18 – 31, Los Alamitos, CA, USA, 2002.

[LT07] T.Y. Liu and W.H. Tsai. A new steganographic method for data hiding in microsoft word documents by a change tracking technique. *IEEE Transactions on Information Forensics and Security*, 2(1):24 – 30, March 2007.

[LT10] I. Lee and W. Tsai. A new approach to covert communication via pdf files. *Signal Processing*, 90(2):557 – 565, 2010.

[NCSC93] United States of America National Computer Security Center. *A Guide to Understanding Covert Channel Analysis of Trusted System.* Number NCSC-TG-030 in NSA/NCSC Rainbow Series. Department of Defense / National Computer Security Center, Fort George G. Meade, Maryland, November 1993.

[NW06] N. Nagatou and T. Watanabe. Run-time detection of covert channels. In *Proceedings of the First International Conference on Availability, Reliability and Security, ARES 2006*, pages 577 – 584, Vienna, Austria, 2006.

[PAK99] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn. Information hiding - a survey. *Proceedings of the IEEE*, 87(7):1062 – 1078, July 1999.

[PK91] P.A. Porras and R.A. Kemmerer. Covert flow trees: A technique for identifying and analyzing covert storage channels. In *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 36 – 51, Los Alamitos, CA, USA, 1991.

[PSCS07] A. Patel, M. Shah, R. Chandramouli, and K.P. Subbalakshmi. Covert channel forensics on the internet: Issues, approaches, and experiences. *International Journal of Network Security*, 5(1):41 – 50, July 2007.

[RGI06] N. Ravi, M. Gruteser, and L. Iftode. Non-inference: An information flow control model for location-based services. In *Proceedings of the 3rd International Conference on Mobile and Ubiquitous Systems*, pages 206 – 215, Piscataway, NJ, USA, 2006.

[RMMG01] P. Ryan, J. McLean, J. Millen, and V. Gligor. Non-interference: Who needs it? In *Proceedings of the 14th IEEE workshop on Computer Security Foundation*, pages 237 –238, Washington, DC, USA, 2001. IEEE Computer Society.

[Rus93] B. Russel. *Introduction to Mathematical Philosophy.* Routledge, 1993.

[Sar06] B. Sartin. Anti-forensics - distorting the evidence. *Computer Fraud and Security*, 2006(5):4 – 6, May 2006.

[SC99] S. Shieh and A.L.P. Chen. Estimating and measuring covert channel bandwidth in multilevel secure operating systems. *Journal of Information Science and Engineering*, 15(1):91 – 106, 1999.

[SK06] M. Smeets and M. Koot. Research report: Covert channels. Master's thesis, University of Amsterdam, February 2006.

[SKJ09] K.E. Sabri, R. Khedri, and J. Jaskolka. Verification of information flow in agent-based systems. In G. Babin, P. Kropf, and M. Weiss, editors, *Proceedings of the 4th International MCETECH Conference on e-Technologies*, volume 26 of *Lecture Notes in Business Information Processing*, pages 252 – 266. Springer Berlin / Heidelberg, May 2009.

[Sri06] S. Srinivasan. Security and privacy in the computer forensics context. In *Prooceedings of the 2006 International Conference on Communication Technology*, page 3, Piscataway, NJ, USA, November 2006. IEEE Computer Society.

[SS93] G. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Science*. Springer-Verlag, 1993.

[TJ10] Z. Trabelsi and I. Jawhar. Covert file transfer protocol based on the ip record route option. *Journal of Information Assurance and Security*, 5(1):64–73, 2010.

[VH06] M. Van Horenbeeck. Deception on the network: Thinking differently about covert channels. In *Proceedings of the 7th Australian Information Warfare and Security Conference*. 174 - 184, December 2006.

[VS97] D. Volpano and G. Smith. Eliminating covert flows with minimum typings. In *Proceedings of the 10th Computer Security Foundations Workshop*, pages 156 – 168, Los Alamitos, CA, USA, 1997.

[Wil10] C. Williams. Russian spy ring bust uncovers tech toolkit. The Register, June 29, 2010.

[WW90] R.J. Wilson and J.J. Watkins. *Graphs: An Introductory Approach*. Wiley, New York, January 1990.

[ZAB07] S. Zander, G. Armitage, and P. Branch. Covert channels and countermeasures in computer network protocols. *IEEE Communications Magazine*, 45(12):136 – 142, December 2007.

[ZLSN05] X. Zou, Q. Li, S. Sun, and X. Niu. The research on information hiding based on command sequence of ftp protocol. In *Proceedings of 9th International Conference on Knowledge-Based Intelligent Information and Engineering Systems*, volume 3683 of *Lecture Notes in Computer Science*, pages 1079–1085. Springer Berlin / Heidelberg, 2005.