Applications of Secure Multiparty Computation: Robotics as a Case Study

Thesis submitted in partial fulfillment
of the requirements for the degree of

MASTER of SCIENCE by RESEARCH
in
COMPUTER SCIENCE

by

SARAT CHANDRA ADDEPALLI
200605021
sarat_a@research.iiit.ac.in

CENTRE for SECURITY, THEORY and ALGORITHMS RESEARCH
International Institute of Information Technology
Hyderabad - 500 032, INDIA
DECEMBER 2009

International Institute of Information Technology
Hyderabad, India

CERTIFICATE

It is certified that the work contained in this thesis, titled "Applications of Secure Multiparty Computation: Robotics as a Case Study" by Sarat Chandra Addepalli, has been carried out under my supervision and is not submitted elsewhere for a degree.

Date	Advisor: Dr. K. Srinathan

To My Parents and Brother

Acknowledgments

Acknowledgements goes here ...

Abstract

Abstract goes here ...

Contents

List of Figures

Figure Page

List of Tables

Chapter 1

Introduction

Introduction goes here...

1.1 First Section

Text of section 1 goes here...

This is to insert a table

This is to insert a figure

1.2 Second Section

Text of section 2 goes here...

Few suggestions

Method	Frobnability
Theirs	Frumpy
Yours	Frobbly
Ours	Makes one's heart Frob

Table 1.1: Results. Ours is better.

1.2.1 Mathematics

Please number all of your sections and displayed equations. It is important for readers to be able to refer to any particular equation. Just because you didn't refer to it in the text doesn't mean some future reader might not need to refer to it. It is cumbersome to have to use circumlocutions like "the equation second from the top of page 3 column 1". (Note that the ruler will not be present in the final copy, so is not an alternative to equation numbers). All authors will benefit from reading Mermin's description of how to write mathematics (see math.pdf).

1.2.2 Footnotes

Please use footnotes[1] sparingly. Indeed, try to avoid footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence). If you wish to use a footnote, place it at the bottom of the column on the page on which it is referenced. Use Times 8-point type, single-spaced.

1.2.3 References

List and number all bibliographical references in 9-point Times, single-spaced, at the end of your paper. When referenced in the text, enclose the citation number in square brackets, for example [2]. Where appropriate, include the name(s) of editors of referenced books.

1.2.4 Illustrations, graphs, and photographs

All graphics should be centered. Please ensure that any point you wish to make is resolvable in a printed copy of the paper. Resize fonts in figures to match the font in the body text, and choose line widths which render effectively in print. Many readers (and reviewers), even of an electronic copy, will choose to print your paper in order to read it. You cannot insist that they do otherwise, and therefore must not assume that they can zoom in to see tiny details on a graphic.

Referring to [1], we state that so and so.

1.2.5 Color

Color is valuable, and will be visible to readers of the electronic copy. However ensure that, when printed on a monochrome printer, no important information is lost by the conversion to grayscale.

For more suggestions to improve your document, see preparationGuide.pdf

[1] This is what a footnote looks like. It often distracts the reader from the main flow of the argument.

Chapter 2

Chapter Name

2.1 SMPC Primitives

2.1.1 Oblivious Transfer

2.1.2 Shamir's Secret Sharing

This SMPC primitive addresses the following problem: suppose a group of treasure hunters would like to lock a safe in such a way that it can't be opened unless there are atleast five (say) of them present at any given time. How many locks and keys would be required for this?

In [3], Shamir proposes a way of sharing a secret among n players, such that any k or more players can reconstruct the secret, but no set of $k-1$ or less players can do so. This is called a (k, n) *secret sharing scheme*, and is achieved by using $k-1$ degree polynomials as described follows:

Require: A player has a secret value v which he has to share
  select a random number r
  $f(x) = v + r_1 x + r_2 x^2 + \ldots + r_{k-1} x^{k-1}$
  for all players i **do**
    send the value $v_i = f(i) = v + r_1 i + r_2 i^2 + \ldots + r_{k-1} i^{k-1}$ to player i
  end for
Ensure: each player i has a share v_i of the secret v

Algorithm 1: On sharing a secret

The player who wishes to share a secret first chooses a $k-1$ degree secret random polynomial (by choosing the $k-1$ coefficients r_1 to r_k), say $f(x)$, and sets the constant term to the value of the secret. He then calculates the value of the "share" to be sent to each player i, as $f(i)$. With this, it is ensured that each player has a "share" of the secret, which he may reconstruct if and only if atleast $k-1$ other players are willing to do so.

Notice, that a $k-1$ degree polynomial's equation can be reconstructed with the knowledge of any k points on the curve (as in the case of any k players colluding), but any set of $k-1$ or less points will

yield no information about the equation of the curve (which means that any set of $k-1$ players or less will not be able to reconstruct the secret!), and thus the objective is achieved.

2.1.2.1 Secret Addition

2.1.2.2 Secret Multiplication

2.1.3 Privacy Preserving Union

Chapter 3

Chapter Name

3.1 Introduction to Robotics

3.2 Problems in Robotics

3.3 Localization

3.4 Global Localization

Chapter 4

Chapter Name

Chapter 4 goes here ...

Chapter 5

Conclusions

Conclusion goes here ....

Related Publications

Bibliography

[1] A. Alpher. Frobnication. *Journal of Foo*, 12(1):234–778, 2002.

[2] Authors. The frobnicatable foo filter. 2006. ECCV06 submission ID 324. Supplied as additional material `eccv06.pdf`.

[3] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22:612–613, 1979.