



**MACQUARIE UNIVERSITY
DEPARTMENT OF COMPUTING
TECHNICAL REPORTS**

**Computing Postgraduate (Research)
Mini Conference 2007
Research Students in Computing**

Department of Computing
Division of Information and
Communication Sciences
Macquarie University
NSW 2109 Australia

Report No. C/TR06-02
June 2007

FOREWORD

The University requires the progress of each Postgraduate (Research) student in the PhD and Masters programs to be formally reviewed every year. To complement the formal University review process, the Department of Computing holds an annual mini-conference for Postgraduate (Research) students. The mini-conference gives the students an opportunity (1) to present their research work to their peers and academic staff, (2) to assess their own progress and research directions, and (3) to discuss all aspects of their program with a panel of academic staff who are not involved in their supervision.

This year's main mini-conference was held between 18-22 June 2007 and the Language Technology Postgraduate Mini-conference is from 14 June to 19 June. This technical report demonstrates the range and depth of the research projects undertaken by Computing Postgraduate (Research) students.

Thanks are due to Lee Flax for the organisation of the mini-conference itself, and Mark Dras for organising the Language Technology Postgraduate Mini-conference and Computing Technical Support for the arrangement of the equipment used in the presentations, Melina Chan for compiling the conference materials and organising the catering, and all the academic staff who participated as panel members, and as members of the audience.

But most particularly I'd like to thank the Postgraduate (Research) students whose excellent research work continues to make these events a success.

Annabelle McIver
Director of Postgraduate Research
Department of Computing
Division of Information and Communication Sciences
Macquarie University

**COMPUTING POSTGRADUATE (RESEARCH) MINI-CONFERENCE
18 -22 JUNE 2007, MACQUARIE UNIVERSITY, AUSTRALIA
and
LANGUAGE TECHNOLOGY POSTGRADUATE MINI-CONFERENCE
14- 19 JUNE 2007**

**LT POSTGRADUATE MINI-CONFERENCE
14- 19 JUNE 2007**

Schedule of Presentations on 14 June 2007 in E6A102

Presentation Time	Speaker	Institution
9:30 - 9:50	Elena Akhmatova	Macquarie University
9:50 - 10:10	Mary Gardiner	Macquarie University
10:10 - 10:30	Matt Honnibal	External
10:30 - 10:50	Andrew Lampert	Macquarie University
MORNING TEA		
11:20 - 11:40	Tara McIntosh	External
11:40 - 12:00	Vanessa Long	Macquarie University
12:00 - 12:20	David Vadas	External
LUNCH		
1:40 - 2:00	Stephen Wan	Macquarie University
2:00 - 2:20	Jim Yaghi	Macquarie University
2:20 - 2:40	Simon Zwarts	Macquarie University
2:40 - 3:00	Luiz Pizzato	Macquarie University
AFTERNOON TEA		
3:30 - 3:50	Toby Hawker	External
3:50 - 4:10	Yefeng Wang	External
4:10 - 4:30	Yitao Zhang	External

**LT POSTGRADUATE MINI-CONFERENCE
14- 19 JUNE 2007**

Abstracts of Presentations –from Macquarie University students

Title: RTE for Entailment Pairs Subtypes
Speaker: Elena Akhmatova

Abstract:

Recognizing Textual Entailment (RTE) is a task where, given two text snippets, the goal is to determine whether the meaning of one text snippet can be inferred from the meaning of the other. The first of the text snippets in such a pair is referred to as the text and the other one as the hypothesis. The pair of text and hypothesis is called an entailment pair. The majority of the state-of-art approaches to textual entailment focus on defining a generic approach to RTE. Though the generic approach is worth pursuing, it was noticed earlier that entailment pairs are different, and an approach for recognition of one type of entailment pairs might not be suitable or effective for another type of entailment pairs. In my work I focus on solving the task of RTE for particular types of entailment pairs. In this talk I present one subtype of entailment pairs that is problematic for existing systems. I'll define this type and present a machine learner to demonstrate the recognisability of the type. Then I'll talk about a two-part probabilistic model for their classification into true and false entailments and the evaluation methods for such an approach.

Title: Treating paraphrase in the context of a training simulation
Speaker: Mary Gardiner

Abstract:

My project aims to use techniques from paraphrase acquisition—the automatic or semi-automatic learning of phrases that mean approximately the same thing—and sentiment analysis—automatic or semi-automatic discrimination of emotional aspects of a text—to acquire near-paraphrases that vary in sentiment from each other. My initial investigations have focussed on whether corpus statistics approaches to discriminating between near-synonyms have any merit, and I've shown that they do so. My talk will briefly discuss this result in the context of my PhD project as a whole and I will then outline my current understanding of my future research programme.

Title: Managing Obligations and Commitments in Email
Speaker: Andrew Lampert
Supervisors: Professor Robert Dale
Co-Supervisor: Dr Cecile Paris (CSIRO)
Associate Supervisor: Dr Steve Cassidy

Abstract:

The volume of textual conversation, including email, web forum discussions, and instant messaging is growing rapidly. This conversational data differs from written documents. It involves interaction between multiple participants, and its structure includes patterns borrowed from verbal conversation. Despite these differences, many search engines and email systems treat textual conversation as simple bags-of-words. Conversational structure is not exploited when searching, navigating or summarising.

Our vision is to provide intelligent, automated assistance to email users. We are developing tools to identify actionable obligations and commitments, drawing on ideas from Speech Act Theory, to assist with the task of email triage in the workplace. Towards this goal, we present findings of an initial experiment building a statistical speech act classifier, using the Verbal Response Modes (VRM) taxonomy of speech acts.

Title: A Blackboard Based Framework for Improving Table Analysis
Speaker: Vanessa Long

Abstract:

The goal of my research is to develop methods for processing tabular data embedded in written documents. One of the main tasks is to search for answers to a long-outstanding question - how to improve table analysis performance?

In this talk, I will discuss a blackboard based framework that has two main advantages: the ability to incorporate a wide range of knowledge sources, including linguistic information and domain knowledge, into the problem solving process, and the ability to allow experts (programs that have the solutions, partial or otherwise) to work cooperatively towards the goal of extracting tables.

I will also show how higher table extraction accuracies could be achieved by using the framework.

Title: Statistical Generation of Novel Sentences
Speaker: Stephen Wan

Abstract:

Many professions today rely heavily on the ability to sift through large volumes of textual documents in order to glean relevant information required for some task. Summarisation technology can provide assistance in helping to identify more accurately which documents are really worth reading in order to extract the relevant information. Current summarisation methods simply extract a disjoint list of sentences deemed as important. However this is far from the ideal of a readable coherent summary passage that humans are able to construct. Ultimately, an automatically generated summariser would rewrite these extracted sentences, creating an abstract-like summary. To this end, this research focuses on creating novel paraphrase sentences. We note that summary sentences may be made up of recycled fragments of text taken from the important sentences in an input document. To combine these recycled words and phrases, we utilise the strengths of both a model of dependencies and an N-gram language model. N-gram models in generation have been

recognised as providing fluency at the level of word sequences. At a higher sentence level, using a statistical syntactic dependency model allows one to represent linguistic phenomena such as long-distance relationships. In our hybrid approach for ordering words, we show that it is possible to improve both the grammaticality of generated word sequences.

Title: Context Sensitive Paraphrasing
Speaker: Jim Yaghi

Abstract:

A context-based paraphrase system is described with application as a teaching tool for the logic course taught in the popular textbook "Language Proof and Logic". Students of the textbook currently can submit their attempts at exercises to an automatic grading facility which gives basic feedback on the correctness of their answers. We aim to give natural language feedback that focuses a student's attention on the errors present in their first order logic responses.

For this, we build natural language paraphrases of the incorrect user input, and guide the paraphrase realisation process using such strategies that would make clear what should be corrected by the student. By having that kind of feedback, we believe that the student can learn how to correct his or her own mistakes, and get a better grasp of the concepts.

Title: Learning structural characteristics in Statistical Machine Translation
Speaker: Simon Zwarts

Abstract:

My talk will be about the use of syntax in SMT. Much debated, but syntax in SMT seems to outperform pure SMT systems. I will show such a system of syntax enriched SMT and its effects.

Furthermore I will sketch a path for further use of syntax, where the keypoint is prevention when syntax is hurtful for SMT.

Title: Information Retrieval for Question Answering
Speaker: Luiz Pizzato

Abstract:

Most information retrieval strategies work on the assumption that results should be delivered directly to the end user who with a brief examination will have the ability to discern between relevant and irrelevant results. My PhD research focuses in building a model that allows IR results to be more relevant for the specific task of question answering. In such a system, receiving documents containing extractable answers is likely to be better than receiving documents that just deal with the relevant subject. To approach this problem I have implemented a set of different strategies, one regarding a feedback mechanism and another using a simplified semantic markup. In my talk I will briefly describe both approaches and some of their latest results.

~~~~~ **End of presentations on 14 June 2007** ~~~~~

**COMPUTING POSTGRADUATE (RESEARCH) MINI-CONFERENCE  
18 -22 JUNE 2007, MACQUARIE UNIVERSITY, AUSTRALIA**

**Schedule of Presentations and Interviews in E6A102**

|      | Mon<br>18 June                               | Tue<br>19 June                | Wed<br>20 June                 | Thu<br>21<br>June | Fri<br>22<br>June |
|------|----------------------------------------------|-------------------------------|--------------------------------|-------------------|-------------------|
| 0900 | Cameron McDonald( <b>Pres</b> )              |                               |                                |                   |                   |
| 0930 | Vijaykrishnan Pasupathinathan( <b>Pres</b> ) |                               |                                |                   |                   |
| 1000 | Sourosch Sedaghat( <b>Pres</b> )             |                               |                                |                   |                   |
| 1030 | Tea Break                                    |                               |                                |                   |                   |
| 1100 | Sanka Balasuriya( <b>Pres</b> )              |                               |                                |                   |                   |
| 1130 | PeiShun Wang( <b>Pres</b> )                  |                               |                                |                   |                   |
| 1200 | Qingsong Ye( <b>Pres</b> )                   |                               |                                |                   |                   |
| 1230 | Lunch Break                                  |                               |                                |                   |                   |
| 1300 |                                              |                               |                                |                   |                   |
| 1330 |                                              |                               |                                |                   |                   |
| 1400 |                                              |                               |                                |                   |                   |
| 1430 | Yifan Gao( <b>Pres</b> )                     | Ji Ma( <b>Pres</b> )          |                                |                   |                   |
| 1500 | Tea Break                                    |                               |                                |                   |                   |
| 1530 | Tauseef Gulrez( <b>Pres</b> )                | Sri Madhisetty( <b>Pres</b> ) |                                |                   |                   |
| 1600 | Eric Fassbender( <b>Pres</b> )               | Armin Hezart( <b>Pres</b> )   | Shirley Goldrei( <b>Pres</b> ) |                   |                   |
| 1630 | Susan Bruck( <b>Pres</b> )                   |                               | Matthew Roberts( <b>Pres</b> ) |                   |                   |
| 1700 | Yi He( <b>Pres</b> )                         | Moad Maghaydah( <b>Pres</b> ) | Howard Lovatt( <b>Pres</b> )   |                   |                   |
| 1730 | Stephen McCombie( <b>Pres</b> )              | Akther Shermin( <b>Pres</b> ) | Gillian Miller( <b>Pres</b> )  |                   |                   |

Note: (**Pres**) means presentations  
(**Int**) means Panel interviews

## Schedule of Presentations and Interviews in E6A357

|      | Mon<br>18 June                                    | Tue<br>19 June                   | Wed<br>20 June                    | Thu<br>21 June                     | Fri<br>22<br>Jun |
|------|---------------------------------------------------|----------------------------------|-----------------------------------|------------------------------------|------------------|
| 0900 |                                                   |                                  |                                   |                                    |                  |
| 0930 |                                                   |                                  |                                   |                                    |                  |
| 1000 |                                                   |                                  |                                   |                                    |                  |
| 1030 | Tea Break                                         |                                  |                                   |                                    |                  |
| 1100 |                                                   | Aarhi Nagarajan<br><b>(Pres)</b> |                                   |                                    |                  |
| 1130 |                                                   | Aarhi<br>Nagarajan <b>(Int)</b>  |                                   |                                    |                  |
| 1200 |                                                   |                                  |                                   |                                    |                  |
| 1230 | Lunch Break                                       |                                  |                                   |                                    |                  |
| 1300 | Lunch Break                                       |                                  |                                   |                                    |                  |
| 1330 | Cameron<br>McDonald <b>(Int)</b>                  |                                  |                                   |                                    |                  |
| 1400 | Vijayakrishnan<br>Pasupathinathan<br><b>(Int)</b> |                                  |                                   |                                    |                  |
| 1430 | Sourosh<br>Sedaghat <b>(Int)</b>                  | Yifan Gao <b>(Int)</b>           |                                   |                                    |                  |
| 1500 | Lunch Break                                       |                                  |                                   |                                    |                  |
| 1530 | Sanka<br>Balasuriya <b>(Int)</b>                  | Tauseef<br>Gulrez <b>(Int)</b>   | Sri<br>Madhisetty <b>(Int)</b>    |                                    |                  |
| 1600 | PeiShun<br>Wang <b>(Int)</b>                      | Eric Fassbender<br><b>(Int)</b>  | Armin Hezart<br><b>(Int)</b>      | Shirley<br>Goldrei <b>(Int)</b>    |                  |
| 1630 | Qingsong Ye <b>(Int)</b>                          | Susan Bruck <b>(Int)</b>         |                                   | Matthew<br>Roberts<br><b>(Int)</b> |                  |
| 1700 | Majid<br>Alkhwati <b>(Pres)</b>                   | Yi He <b>(Int)</b>               | Moad<br>Maghaydah<br><b>(Int)</b> | Howard<br>Lovatt <b>(Int)</b>      |                  |
| 1730 | Majid<br>Alkhwati <b>(Int)</b>                    | Stephen<br>McCombie <b>(Int)</b> | Akther<br>Shermin <b>(Int)</b>    | Gillian<br>Miller <b>(Int)</b>     |                  |

Note: **(Pres)** means presentations  
**(Int)** means Panel interviews

**COMPUTING POSTGRADUATE (RESEARCH) MINI-CONFERENCE  
18 -22 JUNE 2007, MACQUARIE UNIVERSITY, AUSTRALIA**

*Abstracts of Presentations (in alphabetical order of speakers' surname)*

~~~~~

Title: Monitoring and management Business collaboration base on service level

Speaker: Majid Alkahwati

Abstract:

Businesses establish relationship between them to exchange the service through the internet, where some business request service and other provide the service, specifying the roles of each party, what is the format of the messages exchange to provide the service and what is the more important which are the temporal and order constraint for the sequencing of the messages.

Businesses exchange the services need to agree on the service to provide by one business to other before they exchange it. This agreement must to be specified and both businesses sign it.

Agreement defined set of activities, roles, and responsibilities to be taken by different parties to satisfy the terms and conditions in the agreement.

Agreement build a new business relationship between contractual partners and provides a guarantee to all contractual partners according to the clauses of the signed contract and relevant laws.

Monitoring the service exchange and fulfill the agreement to provide the service quality as specified in the agreement, service exchange is set of messages send from party to other, checking the message behavior is the key point of monitoring the service provide, the qualities of each message must specify in the contract, like the message availability, message response time, message order and message usability are the qualities must check on the exchange message.

Not all the messages need to check all the qualities, some messages need to check some of the qualities and other may need to check all the qualities, so we need to classify the message base on message purpose, like the quality need to check on request action message different than the quality check on response message.

In the agreement we can specify exact quality of some messages like response time (when the message should be send), but some qualities we can't specify them in the agreement like throughput quality, because to check the throughput of the message, it is related to the other message, like request information/service and response message, the amount of information/service in the response message will be related to the request message, then I specify in the agreement the service status after message send and during the service exchange, we check this status with the service exchange after this message sent.

I use state machine to check the message behavior, where the messages are the transit between the states and the states are the status after sending the

messages, so in this state machine there is no event in the states, the event will be in the transit.

In this state machine, to check the message quality, I will check the state after this message.

I will have two state machines, one is the contract where it contain all the messages suppose to send and the states qualities after each message, the second machine is the service exchange which contain the actual message sent and the states qualities after each message. Monitoring system will check the states qualities in the two machines.

Title: Security Framework for Wireless Mobile Ad-hoc Networks

Speaker: Venkatesan Balakrishnan

Abstract:

Security is paramount in wireless mobile ad hoc networks as they are not conducive to centralized trusted authorities. At present there are several efforts to secure the communications but they are not designed to evaluate the trustworthiness of communicating devices. Further, there is no suitable security framework that integrates a trust model with a secure routing model. My research thesis focuses on the theory, design, and framework for a secure wireless mobile ad hoc network. Our comprehensive trust enhanced security framework defines the integration of a novel obligation-based fellowship and reputation-based trust models with a secure routing model.

Title: Bounds of Character Sums and Exponential sums

Speaker: Sanka Balasuriya

Abstract:

This talk titled ***Bounds of Character Sums and Exponential sums*** is mainly concerned with the progress and the general direction of the intended research. The character sums and their bounds which play an important part in this research will be discussed. In particular character sums involving some important arithmetic functions will be discussed. A discussion about non-trivial upper bounds of some exponential sums too will be included.

Title: Virtual reality immersive environments and their role in the management of motion sickness.

Speaker: Susan Bruck

Principal Supervisor: Professor Mike Johnson

Associate Supervisor: Senior Lecturer Peter Bull

Adjunct Supervisor: Dr Lee Flax

Abstract

Virtual reality immersive environments are safe, reproducible forums to test an individual's physiological and psychological responses. Identifying virtual reality immersive environments that cause discomfort in specific population groups will provide the opportunities to predict who may be vulnerable in

particular situations. Quantitative and qualitative measures of responses will provide much needed information for educational and clinical professionals who diagnose and treat children with motion sensitivity disorders. The research data will also offer the potential to more effectively recruit and train personnel in industries that use head mounted displays and virtual training environments.

Title: Improved Abstractions for Programming Language Processor Specification

Speaker: Shirley Goldrei

Supervisor: A/Prof Tony Sloane

Associate Supervisor: A/Prof Dom Verity

Abstract:

Two common abstractions for describing computations on trees are Attribute Grammars and Term Rewriting. Both abstractions are frequently described in the research literature as being amenable to the description of the semantics of programming languages. Each of these abstractions have strength and weakness. In particular the strengths of Attribute Grammars is in describing the analysis tasks required to be performed such as checking for programmer errors and computing context sensitive information in general. On the other hand Term Rewriting is particularly convenient for transforming abstract syntax trees to alternate intermediate representations or for expressing optimisations.

In practice, compiler writers very rarely use either of these abstractions preferring to directly hand code analysis and transformation tasks using one or other general purpose programming language. This stands in contrast to abstractions used to describe programming language syntax, where practitioners routinely use syntax definition formalism including well known systems such as Lex and Yacc to describe their language syntax and to generate a parser for the language automatically.

It may be reasonable to conclude then that neither Attribute Grammars nor Term rewriting on their own offers an abstraction that matches the problem of semantic description sufficiently well enough to provide a satisfactory return on investment (i.e. investment in learning to use the domain specific language implementing the abstraction).

Our aim is to improve this situation. In this talk, I will describe some steps I am taking to combine Attribute Grammars and Term Rewriting into a single abstraction which I claim will preserve the advantages of both abstractions.

Title: Body Machine Interface - Remapping the Residual Motor Space of Spinal Cord Injured (SCI) Patients to Control Robotic Devices

Speaker: Tauseef Gulrez

Abstract:

Here I present a novel framework allowing spinal cord injured patients to control a powered wheelchair through signals derived from the patient's residual mobility. The main novelty of this approach lies in substituting the

typical joystick controllers of powered wheelchairs with a sensor shirt. This allows the whole upper body of the patient to operate as an adaptive joystick. With the exception perhaps of the most severe cases, mobility lost to spinal injury can be partially recovered by remapping the redundant degrees of freedom that remain available to the patients. Considerations about risks, particularly for the spinal cord injured population, have lead us to develop a safe testing environment in 3D Virtual Interactive Simulations of Reality (VISOR). VISOR augmented with humans, allows us to analyse learning skills and give patients an adequate training to control a simulated wheelchair through the signals generated by body motions in a safe environment. Our goal is to adapt the control of the wheelchair to the degrees of freedom that patients are most capable to coordinate. This leads to a design that is both custom-oriented and time-varying. We provide a description of the basic theory, of the development phases and of the operation of the complete system. We also present results obtained from subjects using upper body postures to control the simulated wheelchair.

Title: Unresolved issues in Defeasible-Argumentation-Systems

Speaker: Armin Hezart

Supervisor: Dr. Abhaya Nayak

Abstract:

Defeasible argumentation systems are one of the approaches to model non-monotonic reasoning. Argumentation systems have been connected to a wide range of applications including Planning, Automated-Negotiation, Legal reasoning and Commonsense reasoning. The desire to apply Argumentation theory to such wide range of applications has resulted in a number of puzzling and unresolved issues. In this presentation we look at a brief introduction to Argumentation Theory as well as discussing a few of these unresolved issues.

Title: Managing Supportability in Large Software Projects

Speaker: Bruc Lee Liong

Abstract:

There are two parts of software development that are difficult to manage. The first is the development of software itself; the second is the maintenance of the software. Ensuring the software exhibits certain features/properties that would help in both software development and maintenance is topic of this research. The approach proposes an architectural perspective of software development alongside of supplied metrics and tool to ensure that the supportability property (understandability, maintainability, and scalability) is well maintained.

Title: Formal Theories of Trust for Secure Systems

Speaker: Ji Ma

Abstract:

This project focuses on the study of formal theories of trust for secure systems. A theory of trust for a given system is a set of rules that describes trust of agents in the system. Such theories provide a foundation for reasoning about agent beliefs as well as security properties that systems may satisfy. However, trust changes dynamically. When agents lose their trust or gain new trust in a dynamic environment, the theory based on the initial trust of agents needs to be revised, otherwise it may no longer be used for any security purpose. There is a need to provide formal methods for modelling trust of agent in the security mechanisms of a system. The motivation of our work is to provide a formal approach for (design) obtaining and managing evolving theories of trust for agent-based systems. It involves the development of prototype secure systems in selected target applications.

Title:

Speaker: Sri Madhisetty

Abstract:

Utility Computing is an on-demand scalable method of delivering IT services to the business users remotely. Utility Computing delivers its applications as services to its client. As the very nature of computing is become more and more ubiquitous, a licensing model which allows disparate sources to store and process data independently will fast become obsolete.

A much more efficient model which will have a metered access to its services in regards to what services a client would use and bill accordingly will become acceptable. Since these services are delivered remotely there is no technical infrastructure at the clients business to maintain. This research discusses the adoption of such a technology and what are the inhibiting factors.

Title:

Speaker: Moad Maghaydah

Abstract:

XML Management Systems (XMLMS) are emerging as complete systems that can store XML documents and support operations on dynamic XML data like querying, insertions, merging and updates. In both type of XMLMS; Native XMLMS and RDB XMLMS, the XML nodes are identified labelled. The Dewey based labeling method, which is used in some XML data Management Systems, has been considered to be the most suitable technique to support dynamic XML documents. I am presenting a new adaptable and space-efficient labeling technique, called PoD (Prefixing on Demand), based on Dewey identifiers. My technique minimizes the total label size that is generated for general XML documents while maintaining the document order. Furthermore, it supports insertion without relabeling any existing node by providing a parameterized insertion mechanism. My technique also eliminates the need for the complex variable-length prefix-free algorithm that is used in many other proposed solutions. We also report on experimental label length

evaluation between our approach and a *recent Dewey based approach, namely ORDPATH, using well-known XML benchmarks.*

Title: A Specification Framework for Enhanced Information and Logical Modeling

Speaker: Gillian Miller

Abstract:

The aim of my research is to come up with a framework for enhanced data modeling and constraint specification by information systems practitioners. The research is motivated by practical application, but at the same time seeks firm theoretical underpinnings. As part of the framework I have proposed an abstract language to augment models with expressive specification of queries, data structural constraints and invariants that correspond to semantic business rules. The framework is built on a small core model (to unify various information and logical data models) which has a conceptualization as a graph (nodes and multi-headed arrows). Some of the novel features of the framework include a rich set of encapsulated constraint primitives, concept classification and commuting constraints intertwined with a powerful navigation based path language. The result is a small elegant system which allows for the concise representation of commonly occurring constraints. In the talk I will summarize the overall approach. I have also been recently exploring metamodeling (and metametamodeling) as these areas provides interesting application data for the proposed framework.

Title: Techniques for the Design of Trust Enhanced Secure Applications

Speaker: Aarthi Nagarajan

Abstract:

Web services are increasingly being used in daily life for electronic commerce. These services can range from simple requests to complex business processes, but there is still a major concern about the trustworthiness of these services. Although there are standards for providing confidentiality, integrity and authentication of web services, there are no standard techniques available for reasoning the trust levels of such services. This research aims to provide a Trust enhanced Secure Model (TeSM) that will provide means for specifying and managing trust for web based applications.

This talk will address what the present Web Services Trust specification is about and how can Trusted Computing be leveraged to provide trust for web services. In particular, we will talk about trust negotiation and policy support required for trust negotiation using trusted platforms in web services.

Title:

Speaker: Vijayakrishnan Pasupathinathan

Supervisor: Josef Pieprzyk and Huaxiong Wang

Research Title: Functional Cryptographic Protocols

Abstract:

Functional Cryptographic Protocols (FCP) include protocols such as electronic voting, electronic commerce, identity based systems and other application level services that depend on core cryptographic protocols like key establishment, agreement and management, key recovery and escrow, and zero-knowledge systems. The presentation this year consist of our findings on Chuam's evoting , existing first generation passport standard and EU-IACO proposal for second generation passports.

Title: An operational semantics for the pattern calculus
Speaker: Matthew Roberts

Abstract:

Last time, we saw the semantics of the pure pattern calculus from 10,00 feet. This time we dive in to take a closer look. However, rather than describe the pure pattern calculus, we will cover the semantics of our new core language for pattern calculus expressions. It is familiar to those who have seen the pattern calculus and exposes lots of interesting new nooks and crannies that need investigating. We won't have time to look into all them, but I hope at least to rouse your curiosity. I will describe the basic core language and the reasons for many of the design decisions.

Title: Learning Dynamic Bayesian Networks from cDNA Microarray Gene Expression Data
Speaker: Akther Shermin

Abstract:

The reverse engineering of gene regulatory networks using Dynamic Bayesian Network (DBN) suffers from the curse of dimensionality. One way to mitigate this problem is to narrow down the number of potential regulators of each target gene. In our study, we have proposed improved threshold values to identify the time points when a gene is expressed, that is, when it may have influence on the activation or repression of other genes. The use of this expression information has made possible to focus on the most relevant genes as potential regulators of a target gene, which consequently has alleviated both the number of false positive connections and the computation cost of the learning algorithm. In addition, using our revised DBN model we have analysed two new microarray datasets which contain more information about the underlying gene regulatory network than those used in the previous studies

Title: Private Information Retrieval
Speaker: Peishun Wang

Abstract:

A Private Information Retrieval (PIR) protocol allows a user to retrieve a data item of his choice from a database while hiding the identity of the item from the database server. To date, PIR has received significant attention in the literature, and most PIR schemes assumed that the user knows the physical address of the sought item. However, it is usually not the case in most databases in the real world. Instead, the user typically holds a keyword (for example, the name of a specific company traded in the stock market). I tackled this problem, and researched on secure keyword search on encrypted data.

The first problem I solved is to remove the requirement of keyword fields in secure indexes and trapdoors, and constructed a new protocol to solve it. Then, I worked on cryptographic dynamic accumulators, and got a new design with new function -- batch update. Since existing secure search schemes are between a single-user and a server, I extended a single-user setting to a multi-user setting, and constructed a new searchable encryption scheme: common secure indexes for groups. Also, I initiated a new research topic: secure searches for conferences, and created a new scheme on it. Currently I am studying the pairing-based cryptography, and a new protocol of Private Information Retrieval (PIR) based on pairing is being constructed.

Title: Distributed Oblivious Polynomial Evaluation and Privacy-Preserving Set Operations

Speaker: Qingsong Ye

Thesis Title: Enhancing Privacy in Public Information Retrieval

Supervisors: Dr Huaxiong Wang and A/Prof Mehmet Orgun

In this talk, I will present my recent results on privacy-preserving distributed set operations. Our approach is based on our observation on distributed oblivious polynomial evaluation which relies on homomorphic encryption and secret sharing. This solution provides information semantic security and requires no private key to perform computation on encrypted data. Our construction may be of great value for database outsourcing because the privacy of unencrypted data stored in single server is major concern in such a setting.