

isi UPDATE

ISSUE 5 | SEPTEMBER 2010

NEWSLETTER OF THE INFORMATION SECURITY INSTITUTE



Mr Eric Hall,
General Manager
and Director
of Business
Development

from the directors

Biannual Directors Report – August 2010

We have in recent times borne witness to the most hideous elements of the modern social networking phenomenon. Social networking websites are being used on a daily basis for vicious cyber bullying, and for smear campaigns that make a laughing stock of our defamation laws. The social networking phenomenon has facilitated the publishing of information, including lies and innuendo, where a remedy to the average citizen is complicated by the technology and by laws which have not fully adapted to the digital paradigm. No

doubt, there is an upside to the ability to communicate so effectively with an audience, but it is not unreasonable to expect that new technology should avoid introducing new risks and safety concerns into our families' lives.

The Information Security Institute is committed to the creation of new knowledge in the area of cyber safety. It is recognised that this is not a one dimensional problem. Issues arise in sociology, criminology, regulatory and legislative frameworks, not to mention the influence technologists can have in designing systems that inherently mitigate the risks involved. The Institute is leading a national bid for the establishment of a Cooperative Research Centre in Resilient Cyber Systems. The Centre, if funded, will explore the prevention of anti-social attacks in social networking sites, social networking safety for minors, consumer-legal issues in cloud computing and human factors in resilient cyber systems. This is in addition to large information security challenges such as critical infrastructure protection, digital forensics, biometrics and risk management.

This multidisciplinary approach is in keeping with the original philosophy behind the establishment of the Institute – we draw on expertise from Engineering, Science, Technology, Law and Business. While this may not always be the best way to frame a traditional ARC Discovery grant, this is the only way to develop holistic solutions that will work in practical applications. We need to extend our repertoire, so that we are equally adept in pursuing research opportunities at both ends of the spectrum. That is the practical, applied systems, multidisciplinary approach which QUT has traditionally been very good at, and the more singular discipline focussed ERA approach, which looms around the corner.

new funded projects

- **Department of Prime Minister and Cabinet – National Security Science and Technology Unit (NSSTU),**
 1. Professor Sridha Sridharan [BEE] and Dr Clinton Fookes [BEE] '**Intelligent Surveillance Research for Crowd Monitoring and Event Detection**' three-year project, the total cash funding is \$320 000.
 2. Associate Professor Andrew Clark [FST] and Dr Jason Smith [FST], '**Vulnerability Assessment for Web Services – Phase 2**', one-year project, the total cash funding is \$88 840.
 3. Associate Professor Andrew Clark [FST] and Dr Bradley Schatz [FST], '**Forensic Readiness in Control Systems: Tools and Methods**', one-year project, the total cash funding is \$131 121.
- **ARC Linkage**

Professor Sridha Sridharan [BEE] and Dr Michael Mason [BEE] 'Robust Automatic Speaker Diarisation of Audio Documents by Exploiting Prior Sources of Information' four-year project, the total cash funding is \$394 245. Industry partner is Validvoice Pty. Ltd.

in this issue

- 2 **PDL at Supélec, Rennes, France**
Associate Professor Andrew Clark
- 3 **National Risk Assessment – A Tool for Planning Resilience**
Dr Paul Barnes
- Eureka! Computer surveillance scientist wins**
- 4 **Recycling of computing devices: risks to privacy and confidentiality**
Dr Bradley Schatz

isi invited talks at national and international conferences

- Professor Ed Dawson (Keynote): **Information Sharing in the 21st Century: Progress and Challenges**, AISC 2010, Brisbane, Australia, 18–21 January, 2010
- Professor Ed Dawson (Invited): **Elliptic Curves, Group Law and Efficient Computation** presented at The Claude Shannon Institute Workshop on Coding and Cryptography, Cork, Ireland, 17–18 May, 2010
- Dr Clinton Fookes (Keynote): **Semi-supervised Intelligent Surveillance System for Secure environments** presented at IEEE Industrial Electronics Symposium, Special Session on Computational Intelligence for Safe and Secure Environments and Transport, Bari, Italy, July 2010
- Dr Paul Barnes (Keynote): **The National Risk Assessment** to be presented at Safeguarding Australia Threats and Responses Conference, Canberra, 22 September, 2010.
- Associate Professor Andrew Clark (Invited): **A Security Oriented Architecture?** DSD Cyber Security Conference, Canberra, 25 March 2010.

isi best student paper award at international conferences

- Farzad Salim [FST] was presented the Best Student Paper Award for his paper on An Administrative Model for UCON, AISC 2010, Brisbane, Australia, 18–21 January, 2010

VISITORS TO ISI:

Researchers visiting the ISI:

- Dr Michel Abdalla, Computer Science at École Normale Supérieure, Paris, 14–18 March, 2010.
Seminar topic: Robust Encryption Provable Security: What's it all about?
- Professor Roy Maxion, Computer Science Department, Carnegie Mellon University, 19–22 April, 2010.
Seminar Topic: Keystroke Biometrics with Number-Pad Input
- Dr Berkant Ustaoglu, NTT Laboratory, Tokyo, 11–23 March, 2010
Seminar Topic: Off-the-Record Messaging and Privacy Issues in Key Establishment
- Professor Jung-Tae (Steve) Kim, Mokwon University, Daejeon, Republic of Korea, 28 June to 22 August, 2010

Professor Colin Boyd



Professor
Colin Boyd,
Research Director

When ISI first evolved into an institute from a research centre in 2005, four QUT faculties were involved: Built Environment and Engineering; Business; Information Technology; and Law. This did not mean that other disciplines were excluded from information security research, only that the core faculties reflected the strategic directions of ISI. The merger of two QUT faculties into the new Faculty of Science and Technology in 2009 led to new opportunities for ISI to extend collaboration with researchers in various scientific disciplines. One example is the possibility for ISI researchers in computer and network forensics to team up with researchers in chemistry and biology working in forensic science. Another example, the application of mathematics in information security, has recently taken a step forward.

Collaboration with mathematicians has been common for ISI researchers for many years. Perhaps the most obvious area where this has occurred has been in the cryptology group; in fact several members of ISI's cryptology group have a strong mathematical background. However, the potential for collaboration with mathematicians goes well beyond cryptology. In recognition of this potential, and building on the opportunities from the faculty merger, ISI researchers joined with QUT mathematicians for a two-day ISI-Maths workshop in April this year to explore the most effective collaborations. Around 30 researchers were actively involved in the workshop which included a keynote address from Professor Roy Maxion of Carnegie Mellon University. Topics discussed included: information flow, network traffic analysis, data mining, random indexing, network optimisation, image processing, complex systems, computational mathematics, and high performance computing. This list illustrates the range of expertise available to ISI and the potential for the influence of formal modelling and analysis in information security.

Outputs from the ISI-Maths workshop included the identification of a wide range of collaborative project areas where QUT's mathematicians can work together with ISI researchers in different disciplines. Some examples of these are network optimisation (involving network security and mathematical modelling); mining of large data sets (including network forensics and data mining); and risk management. The latter area is currently being taken forward with the support of an ISI seeding grant fund on evaluating resilience in ICT-rich infrastructure, which brings together researchers from the Faculty of Business and mathematicians in the Faculty of Science and Technology. As is often the case with such events, the most valuable output may well be the personal contacts established. The mutual understanding of what ISI researchers across all the disciplines need in terms of mathematical reasoning and how they can work together with the mathematicians have planted the seeds for future collaboration. In the longer term we can expect ambitious projects to be funded to take these seeds to fruition.



Associate Professor
Andrew Clark
Deputy Director, ISI
Leader of the
Network Security
and Digital
Forensics Group

PDL at Supélec, Rennes, France

In the second half of 2009 I was fortunate enough to spend 12 weeks with the Information Systems Security and Networks group (Sécurité des Systèmes d'Information et Réseaux – SSIR) at Supélec (Ecole Supérieure d'Électricité) in Rennes, the capital of Brittany in western France. The group, led by Professor Ludovic Mé, consists of a team of network security and intrusion detection researchers who also teach a popular Masters-level program called 'Information and Computing Infrastructure Security'.

During the visit I worked closely with the team on a project extending the Blare host-based intrusion detection system that has been developed over a number of years at Supélec. Blare is implemented in the Linux kernel and monitors information flows through the kernel to check that they do not violate a given information flow policy. I worked on optimising the kernel implementation to allow the checking of a more fine-grained policy. The outcomes of this work were presented at the 2010 International Workshop on Managing Insider Security Threats in Japan, by Valérie Viet Triem.

The PDL provided an opportunity to meet with a variety of researchers from the European research community both in France (where both the European Symposium on Research in Computer Security, ESORICS, and Recent Advances in Intrusion Detection, RAID, conferences were held) as well as in Norway (at the Nordsec09 conference). My partner Megan and I also took advantage of the fantastic regional foods and markets in Rennes, and a couple of times, spent weekends exploring the majestic Brittany coastline.

Since returning to Brisbane I have continued to develop the strong relationship with the team in Rennes. QUT and Supélec have since entered into an International Collaborative Agreement and are currently working towards the shared enrolment of a PhD student under a cotutelle agreement. It is hoped that in the future the agreement may be extended to include shared recognition of each others' Masters level security courses.

national risk assessment – a tool for planning resilience



Dr Paul Barnes
Deputy Director, ISI
Leader of the
Risk and Crisis
Management Group

In the December 2008 National Security Statement (NSS), Kevin Rudd identified a broad and growing list of threats and pressures in the international system that have the potential to impact on Australia's national interests. In addition to the continuing possibility of state-based conflict, a range of non-traditional and non-state threat sources was highlighted. These included climate change, pandemic diseases, terrorism, organised crime, as well as energy and information security. According to the NSS, a critical element of the national security framework will be to 'make choices concerning the relative priority to be afforded to future national security capabilities and policies'.

Such a focus on national level assessments is becoming a standard issue in international settings, especially in protecting critical infrastructure systems. A growing concern in an interconnected - but by no means integrated - world is that without such attention at the highest level crises can expand and initiate a rapid spread of impacts, geographically and over time, often rendering a comprehensive understanding of the scale and context of impacts beyond the grasp of competent authority. Such events have been described as 'outside of the box', 'too fast', and 'too strange.'

In late 2009 Dr Paul Barnes, Coordinator of the ISI Risk and Crisis Management Research Domain completed a project for the Office of the National Security Adviser and the Australian Strategic Policy Institute benchmarking selected international approaches to National Risk Assessment. From this work a number of converging themes were evident internationally: the first was an increasing application of the concept of resilience and all-hazards assessment

and the second, centralized responsibility for policy development and assessing risk and mitigation options at a federal level. Other practice exemplars included the use of common terminologies and risk assessment methodologies along with coordinated governance arrangements. In addition to reporting on international practice the report recommended arrangements for carrying out comparable national risk assessment in Australia.

The full ramification of national and international crises is often difficult to anticipate or predict. An important goal of strategic risk assessment is to capture the scale and extent (consequences) of disturbances that can result from such crises. A targeted national risk analysis process would allow consideration of incidents impacting a number of areas such as:

- *Built Engineering Lifelines*—transport, water, electricity, gas, and telecommunication (including effects on buildings and infrastructure)
- *Biotic Environment*—water and air quality, security of food chain, ecological disruption, urban ecosystems, agricultural ecosystems, natural ecosystems, reduced biodiversity and habitat loss
- *Social and Economic Lifelines*—food distribution, transport networks, schools, medical services, community health, emergency response capacity, employment, business and production, industrial processes and production, tourism, trade/exports and community safety.

Dr Barnes will present a keynote address on national Risk Assessment, based on this comparative study, at the upcoming Safeguarding Australia Conference in Canberra on 22 September, 2010.

eureka! computer surveillance scientist wins

A Brisbane scientist who is creating technology to keep public spaces safe has been awarded the People's Choice Award in this year's prestigious science awards, the Australian Museum Eureka Prizes.

QUT's Dr Clinton Fookes, from the School of Engineering Systems, studies computer vision for surveillance and biometrics.

Dr Fookes was one of only six finalists chosen from hundreds of entries in the Eureka Prizes for scientific research and innovation.

'My research is about 'making sense' of what computers see,' Dr Fookes said.

'We're now literally surrounded by surveillance cameras, but the amount of capability they give us is almost zero.'

Dr Fookes' research includes developing biometrics which aims to uniquely identify a person using some of their physiological or behavioural traits.

He is utilising computer vision to recognise and report on people, objects and their actions to improve our security in public places.

'We are seeking ways to automatically extract and interpret important information from visual sources, including images and video,' he said.

'Research in this field could lead to new discoveries in a range of areas including human-computer interaction, security, medical imaging and robotics.'

Dr Fookes is also using computer vision to monitor the effectiveness of large-scale engineered systems, like our airports.

The Eureka Prizes People's Choice Award aims to promote science generally and inspire young budding scientists to take up a career in this field.

ABC's *Catalyst* featured about Dr Fookes on August 26.

Inside QUT September, 2010 Issue



Dr Michel Abdalla

VISITING ACADEMICS TO ISI:

Dr Michel Abdalla

Michel Abdalla is a staff researcher (CNRS) in Computer Science at École Normale Supérieure, Paris. From 14 March to 28 March 2010 he made a short visit to the ISI.

Michel spent most of his time collaborating with staff and students of the ISI in the area of cryptography and password authentication. During the visit, he made two presentations: One was part of the ISI seminar series, on the topic of Robust Encryption. The other was a joint ISI and Computer Science Discipline seminar on the topic Provable Security: What's it all about? Michel also led a meeting of the cryptography reading group.

Michel was accompanied by his wife, staying in accommodation close to QUT as a guest of the Institute allowing them to enjoy QUT- Gardens Point campus and the city of Brisbane.

Michel completed his PhD at University of California at San Diego in 2001 under Mihir Bellare, the joint founder of practice oriented provable security. Michel's research focus is in public key cryptography. He has published in all the top security conferences, including Crypto, Eurocrypt, TCC and ESORICS as well as A journals such as Journal of Cryptology and IEEE Transaction on Information Theory. He has been an invited speaker at numerous international conferences and was Program Chair for the ACNS conference in Paris in 2009.*

recycling of computing devices: risks to privacy and confidentiality



Dr Bradley Schatz
Adjunct Professor
since 2009.
Research Interests:
Computer Forensics

Assuming that information is kept confidential is one of the trio of fundamental information security goals. At odds with the enduring nature of this goal, is the rapidly evolving ecosystem of digital technologies, and the propensity for information to lodge in unforeseen and unreachable places. With computers becoming embedded within the most familiar of electronic devices, recycling of such devices is fraught with the potential for losses of confidentiality.

In the early mainframe era, means for the assurance of confidentiality could be framed in terms of the location of storage media such as bulky magnetic tapes. The challenge was largely one of physical security.

In the personal computing era, the challenge was reframed by the ease with which information could be copied and relocated using inexpensive floppy disk storage media, or the ease with which information remnants could be retrieved from recycled media. This led to a general awareness within the information technology professions of standard techniques for information destruction and sanitization of media. Despite this, studies over the last decade have consistently showed that confidential and private information is retrievable from the majority of hard drives purchased from the second hand storage market.

Today, the challenge of assuring confidentiality must be reframed both in terms of the propensity for information to lodge in unforeseen and unreachable places, and the extent to which information tends to diffuse throughout a diverse information technology ecosystem. For example, significant difficulties lie simply in recognizing that the office photocopier is potentially a computer with storage capabilities. Recycling of such devices carries with it the potential for revealing stored copies of scanned documents, and authentication credentials used to email scanned documents.

The transformation of mobile phones into powerful portable computers carries similar, but more widespread problems. For example, devices such as the iPhone hold significant amounts of personal information, including emails (and attached documents), usernames, passwords, photographs, and potentially, banking related details.

The extent to which such devices are being recycled while carrying confidential information has to date not been the subject of any widespread study. Research is required towards providing general methods for identifying, accessing, and erasing the storage in such devices, and more generally, in tracking the movement of information across its lifecycle.

For the moment, safely recycling digital devices requires that information managers focus business-wide on all business functions (including those traditionally outside of IT) in order to identify potential storage devices. Effective erasure of such devices remains ad-hoc, generally a matter of trade experience and research, and partly a matter of faith.

Dr Schatz was sought by the *Sun Herald* to comment on privacy risks in disposal of photocopiers (30 May, 2010, p. 35)



completions

PhD

- Saleh Almotairi (FST), *Using Honey pots to Analyse Anomalous Internet Activities*. Supervisors: Associate Professor Andrew Clark (Principal), Professor George Mohay (Associate), Dr Jacob Zimmermann (Associate)
- Marianne Hirschi (FST), *A Multiple Control Fuzzy Vault – A Multiple Control Biometric Cryptosystem with Fingerprints*. Supervisors: Professor Colin Boyd (Principal), Professor Wageeh Boles (Associate)
- Andrew Marrington (FST), *Computer Profiling for Forensic Purposes*. Supervisors: Professor George Mohay (Principal), Associate Professor Andrew Clark (Associate), Dr Hasmukh Morarji (Associate)
- Ejaz Ahmed (FST), *Monitoring and Analysis of Internet Traffic Targeting Unused Address Spaces*. Supervisors: Associate Professor Andrew Clark (Principal), Professor George Mohay (Associate)
- Bander Alhaqbani (FST), *Privacy and Trust Management for Electronic Health Records*. Supervisors: Professor Colin Fidge (Principal), Professor Arthur Ter Hofstede (Associate)
- Choudary Gorantla (FST), *Design and Analysis of Group Key Exchange Protocols*. Supervisors: Dr Juan Gonzalez-Nieto (Principal), Professor Colin Boyd (Associate)
- Huseyin Hisil (FST), *Elliptic Curves, Group Law, and Efficient Computation*. Supervisors: Professor Ed Dawson (Principal), Dr Gary Carter (Associate), Dr Kenneth Wong (Associate)
- David Ross (FST), *Securing IEEE 802.11 Wireless LANs*. Supervisors: Professor Mark Looi (Principal), Dr Andrew Clark (Associate)
- Mehdi Kiani Harchegani (FST), *Systematic Analysis of Anomaly-Based Multi-Model Detection of SQL Injection Attacks*. Supervisors: Associate Professor Andrew Clark (Principal), Professor George Mohay (Associate)
- Reza Z'Abu (FST), *Analysis of Linear Relationships in Block Ciphers*. Supervisors: Professor Ed Dawson (Principal), Leonie Simpson (Associate), Dr Kenneth Wong (Associate), Dr Matt Henderson (Associate)
- Tristan Kleinschmidt (BEE), *Robust Speech Recognition using Speech Enhancement*. Supervisors: Professor Sridha Sridharan (Principal), Dr Michael Mason (Associate)
- Mark Cox (BEE), *Unsupervised Alignment of Thousands of Images*. Supervisors: Professor Sridha Sridharan (Principal), Dr Michael Mason (Associate), Dr Simon Lucey (Industry Supervisor)
- Ivan Himawan (BEE), *Speech Recognition using Ad-Hoc Microphone Arrays*. Supervisors: Professor Sridha Sridharan (Principal), Dr Michael Mason (Associate), Adjunct Professor Iain McCowan (Associate)

Master of Information Technology (Research)

- Reza Hasehzadeh (FST), *A Secure Framework and Related Protocols for Ubiquitous Access to Electronic Health Records Using Java SIM Cards*. Supervisors: Dr Tony Sahama (Principal), Professor Colin Fidge (Associate)

Master of Business (Research)

- Natalie Sinclair (BUS), *Resilience in Critical Infrastructures. The Case of the Queensland Electricity Industry*. Supervisors: Dr Paul Barnes (Principal), Professor Lisa Bradley (Associate)

T - Faculty of Science and Technology

BEE - Faculty of Built Environment and Engineering

BUS - Faculty of Business

ISI 2010 SEED FUNDING GRANTS

- Professor Bill Lane [LAW], Professor Uwe Dulleck [BUS], Dr Jason Reid [ISI], Dr Rouhshi Low [BUS], Mark Burdon [LAW]. Project Title: **A New Legal Framework for the Regulation of Corporate Information Security**. Amount granted \$5000.
- Dr Ejaz Ahmed [FST], Associate Professor Andrew Clark [FST]. Project title: **Assessing the Security Risk of Cloud Computing**. Amount granted \$3000.
- Dr Paul Barnes [BUS], **Measuring and evaluating resilience in complex, ICT-rich infrastructure systems**. Amount granted \$3000.

ISI RESEARCH INCENTIVE SCHEME (IRIS)

- IRIS was introduced in late 2009 to increase the quality level of the journals and conferences on which ISI research is published. The scheme encourages researchers to submit their works to strategically selected conferences and journals.
- To date, the ISI has awarded 18 Conference Travel applications and three Journal Funding Support applications, for a total funding of \$48300.

CONFERENCES:

The ISI hosted the following recent event:

- Australasian Information Security Conference(AISC) held at QUT, Brisbane, 19–20 January, 2010
- India Australia Conference on Information Technology Security (IACITS 10) held at QUT, Brisbane, 13–14 April, 2009
- An Indo/Australian Collaborative DDoS project workshop held at QUT, Brisbane, 15–16 April 2009

graduate destinations

Dr Praveen Gauravaram

Awarded PhD in 2007

Thesis Title: **Cryptographic Hash Functions: Cryptanalysis, Design and Applications**

Supervisors: Dr William Millan (Principal)

Dr Praveen Gauravaram PhD, a graduate from the Information Security Institute and a postdoctoral Research Fellow at DTU Mathematics in Denmark, received the Danish Independent Research Council's Young Elite Researcher's Award 2009 for his research on the analysis of cryptographic hash functions and protocols that use them. The objective of

Praveen Gauravaram's research is to analyse cryptographic hash functions whose security is of prime importance for the secure functionality of cryptographic protocols. In the past few years, Praveen Gauravaram has contributed considerably to the understanding of the security of cryptographic hash functions as well as protocols based on hash functions. For instance, together with Professor Lars Knudsen, he has analysed digital signature security based on randomized hash functions. Some of these results were published at EUROCRYPT 2009, a prestigious conference in cryptology. This research article was awarded one of the three best papers presented at the conference. Praveen Gauravaram is also a successful recipient of a research grant from the Danish Council of Independent Research in 2008 and 2009. In 2009, he was awarded the grant jointly from the Technology and Production Sciences and Natural Sciences of the Danish Council of Independent Research.



Dr Roy Wallace

Awarded PhD in 2010

Thesis Title: **Spoken Term Detection for Audio Mining**

Supervisors: Professor Sridharan (Principal)

Dr Wallace completed his PhD in 2010 and has taken up a two-year postdoctoral position on *Bayesian Networks for face recognition* working with Sebastien Marcel at IDIAP, in Martigny, Switzerland. Dr Wallace 's research will be conducted in the context of a new project funded by the European Community.

The overall goal of the project is to develop new algorithms and models based on Bayesian Networks for unconstrained face recognition. Indeed, the main challenge in face recognition is to account for the possible variations between the face images in the gallery and the probe image. There are many sources of variabilities between two face images of the same individual, including head pose, illumination conditions, facial expression or partial occlusion. State-of-the-art recognition algorithms are capable of correctly recognizing people under controlled conditions, where the face is directly in front of the camera, and with frontal illumination. However, face recognition in an unconstrained environment is still an issue. The research will rely on previous knowledge and software developed at IDIAP www.idiap.ch.



student awards and achievements

- **Chris Doble [FST]** was awarded an ISI Honours Scholarship to undertake his honours project titled: **Data Flow Analysis of Embedded Program Expressions**. The scholarship is valued at \$5000 as a study stipend over two semesters.
- **Ken Radke [FST]** was awarded the Deans Academic Excellence Award for the Graduate Certificate in IT, Faculty of Science and Technology, QUT, Brisbane.

Craig Costello **Current PhD Student**

Thesis Title: **Efficient Implementation of Elliptic Curve Pairings in the Identity-Based Setting**

Supervisors: Professor Colin Boyd (Principal), Dr Juan Gonzalez-Nieto (Associate)



Recipient of the 2010 Fulbright Telstra Scholarship

Craig Costello is the winner of the prestigious 2010 Fulbright Postgraduate Scholarship in Technology and Communications sponsored by Telstra. The scholarship aims to nurture technology and communication professionals '... whose ideas and leadership will shape the future of our world.'

Craig is a graduate from the Queensland University of Technology (QUT) with a Bachelor of Applied Science in mathematics with first class honours in the Dean's Scholars program. Currently, he is undertaking a PhD in the Information Security Institute through an Australian Postgraduate Award, as well as Vice-Chancellor's, Information Technology and Queensland Smart State top up awards.

Based at the University of California (Irvine), from July 2010 he will undertake twelve months' research into new techniques for security on computer and telecommunications devices. 'I will work with world-leaders in an applied field of mathematics known as pairing-based cryptography, which promises to make it possible to improve digital security, particularly on devices with limited computational power such as mobile phones, palm pilots, laptops, remote sensors, and smartcards,' Craig said.

His work will focus on the area termed 'pairings on elliptic curves'. 'Pairings are unique, complex mathematical functions that have very special properties. These pairings have been known to mathematicians for a long time, but their power and potential in the area of cryptography has only been discovered recently.'

Craig plans to use the knowledge gained in the U.S. to develop technology that will benefit all users of electronic communications who require security for their information, including the financial sector, commerce, national security agencies and domestic users.

'Australia's research community will greatly benefit from our results being published at high profile conferences and from the continued collaboration with expert cryptographers in the USA. Many of my colleagues at QUT are researching in this area and my work abroad is likely to influence their research.'

Apart from his academic life, Craig is interested in basketball, tennis, surfing, running, table tennis, golf and chess. He is also currently involved in a voluntary personal project on the Gold Coast that aims to provide gifted mathematics students with the same opportunities he has had, particularly those who aren't exposed to the higher order extra-curricular mathematics that is only offered at a small fraction of high schools.

The prestigious Fulbright program is the largest educational scholarship of its kind, created by U.S. Senator J. William Fulbright and the U.S. Government in 1946. Aimed at promoting mutual understanding through educational exchange, it operates between the U.S. and 150 countries. In Australia, the scholarships are funded by the Australian and U.S. Governments and corporate partners and administered by the Australian-American Fulbright Commission in Canberra.

Craig Costello is one of 24 talented Australians to be recognised as Fulbright Scholars in 2010.

(also cited in *Issue 302, Inside QUT April 2010*, p.5)

