



# RESEARCH FELLOW

DEPARTMENT/UNIT	Department of Software Systems and Cybersecurity
FACULTY/DIVISION	Faculty of Information Technology
CLASSIFICATION	Level A
DESIGNATED CAMPUS OR LOCATION	Clayton campus

## ORGANISATIONAL CONTEXT

---

Everyone needs a platform to launch a satisfying career. At Monash, we give you the space and support to take your career in all kinds of exciting new directions. You'll have access to quality research, infrastructure and learning facilities, opportunities to collaborate internationally, as well as the grants you'll need to publish your work. We're a university full of energetic and enthusiastic minds, driven to challenge what's expected, expand what we know, and learn from other inspiring, empowering thinkers. Discover more at [www.monash.edu](http://www.monash.edu).

The **Faculty of Information Technology** aims to lead global IT research and education. Our strong reputation and international profile attract the best students worldwide and we offer a range of accredited courses that transform our graduates into highly skilled and sought after IT professionals, equipped to work globally. Our research is multidisciplinary, multi-campus and multinational, giving us a unique capacity to reach out further and deeper than any other institution in Australia. Our research priorities are both technically ambitious and embedded in everyday life. To learn more about the Faculty and the exciting work we do, please visit our website: [www.monash.edu/it](http://www.monash.edu/it).

The **Department of Software Systems and Cybersecurity (SSC)** is a world leader in cybersecurity research. As technology becomes more deeply integrated into our everyday lives, the smarter and more alert we need to become. Through our work we seek to understand and address the challenges created by the constant re-imagining of technology. We navigate the ever-changing public perspectives on issues such as privacy and self-disclosure, and the expectation of convenience and trust in online services.

Every individual, business and society who uses online services is exposed to a range of vulnerabilities. Privacy violations, financial fraud and service interruptions, to name a few. That's why we focus on developing sophisticated applications to store, access and manipulate data – to ensure its integrity, reliability and safety.

## POSITION PURPOSE

---

A Level A research-only academic is expected to contribute towards the research effort of the University and to develop their research expertise through the pursuit of defined projects relevant to the particular field of research.

This position forms part of an ARC funded research project on design of efficient cryptographic protocols. It will involve the design and evaluation of high performance implementations of lattice-based cryptographic protocols, including digital signatures, public-key encryption, and zero-knowledge proofs, with security against side-channel attacks.

**Reporting Line:** The position reports to the Chief Investigator

**Supervisory Responsibilities:** Not applicable

**Financial Delegation:** Not applicable

**Budgetary Responsibilities:** Not applicable

## KEY RESPONSIBILITIES

---

Specific duties required of a Level A research-only academic may include:

1. The conduct of research under limited supervision either as a member of a team or, where appropriate, independently and the production or contribution to the production of conference and seminar papers and publications from that research
2. Involvement in professional activities including, subject to availability of funds, attendance at conferences and seminars in the field of expertise
3. Limited administrative functions primarily connected with the area of research of the academic
4. Development of a limited amount of research-related material for teaching or other purposes with appropriate guidance from other staff
5. Occasional contributions to teaching in relation to their research project(s)
6. Experimental design and operation of advanced laboratory and technical equipment or conduct of advanced research procedures
7. Attendance at meetings associated with research or the work of the organisational unit to which the research is connected and/or at departmental, school and/or faculty meetings and/or membership of a limited number of committees
8. Advice within the field of the staff member's research to postgraduate students
9. Other duties as directed from time to time

## KEY SELECTION CRITERIA

---

### Education/Qualifications

1. The appointee will have:
  - An honours degree in the relevant discipline or have equivalent qualifications or research experience; or
  - an honours degree or higher qualifications in the relevant discipline and/or progress towards a doctorate in the relevant discipline; or
  - a doctoral qualification in the relevant discipline or a closely related field.

## **Knowledge and Skills**

2. Demonstrated analytical and manuscript preparation skills; including a track record of refereed research publications
3. Ability to solve complex problems by using discretion, innovation and the exercise diagnostic skills and/or expertise
4. Well-developed planning and organisational skills, with the ability to prioritise multiple tasks and set and meet deadlines
5. Excellent written communication and verbal communication skills with proven ability to produce clear, succinct reports and documents
6. A demonstrated awareness of the principles of confidentiality, privacy and information handling
7. A demonstrated capacity to work in a collegiate manner with other staff in the workplace
8. Demonstrated computer literacy and proficiency in the production of high level work using software such as Microsoft Office applications and specified University software programs, with the capability and willingness to learn new packages as appropriate
9. Demonstrated research experience and skills in high-performance implementation techniques for lattice-based cryptographic algorithms and their evaluation
10. Demonstrated research experience and skills in side-channel resistant implementation of cryptographic algorithms

## **OTHER JOB RELATED INFORMATION**

---

- Travel to other campuses of the University may be required
- There may be a requirement to work additional hours from time to time
- There may be peak periods of work during which taking of leave may be restricted

## **GOVERNANCE**

---

Monash University expects staff to appropriately balance risk and reward in a manner that is sustainable to its long-term future, contribute to a culture of honesty and integrity, and provide an environment that is safe, secure and inclusive. Ensure you are aware of and adhere to University policies relevant to the duties undertaken and the values of the University. This is a standard which the University sees as the benchmark for all of its activities in Australia and internationally.