

# Research Assistance (RA) on Adversarial Machine Learning

AI Security Group @ Macquarie University

**Location:** Sydney, NSW  
**Employment Type:** Casual for 5-6 months.  
**Level:** HEW 7.1 / HEW 5.1  
**Department:** School of Computing  
**Reports To:** Dr Qiongkai Xu  
**Closing Date:** 01/10/2026

## Job Overview

---

The **Research Assistant (RA)** will work at HEW 7.1 / HEW 5.1 and support the AI Security team in conducting research on adversarial machine learning and exploring new defence mechanisms. The role involves data collection, supporting the organisation and delivery of a shared-task competition, conducting research on defence methods, and contributing to research papers, while working closely with CIs Dr Qiongkai Xu and Dr Xuanli He.

## Key Responsibilities

---

The successful candidate will be responsible for:

- Supporting the organisation and delivery of a shared-task competition.
- Conducting frontier research in AI security, with a particular focus on defence methods.
- Contributing to the preparation of research papers and technical reports.

## Essential Criteria

---

Applicants should demonstrate:

- Relevant qualification in Computer Science or equivalent experience.
- Available working visa in Australia.
- Experience in large foundation models, especially vision-language models.
- Demonstrated ability to fundamental machine learning research.
- Strong knowledge in security problems and solutions.
- Strong math and problem-solving skills.
- Strong written and verbal communication skills.
- Ability to work independently and collaboratively.
- Strong organisational and time-management skills.

Applicants should demonstrate:

- A relevant qualification in Computer Science or a related discipline, or equivalent experience. (Candidate with a PhD degree or senior PhD students are preferred.)
- Valid working rights in Australia.
- Experience with large foundation models, particularly vision and language models.
- Demonstrated ability to conduct fundamental machine learning research.
- Strong knowledge of security challenges and defence methods in AI and machine learning.
- Strong mathematical and problem-solving skills.
- Strong written and verbal communication skills.
- Ability to work independently and collaboratively.
- Strong organisational and time-management skills.

## About Us

---

Our team is committed to advancing AI security research and aims to develop secure and trustworthy large foundation models with minimal training and fine-tuning requirements.

## How to Apply

---

Please submit:

- A current CV or résumé;
- A cover letter outlining your suitability for the role; and
- Your recent availability and visa situation.

Applications should be submitted by **01/10/2026**.

For enquiries regarding this position, contact:

**Name:** Dr Qiongkai Xu

**Email:** qiongkai [DOT] xu [AT] mq [DOT] edu [DOT] au