Candidate Information

Position: Research Fellow in Trustworthy AI (2 posts), EEECS
School/Department: Centre for Secure Information Technologies
Reference: 23/111169
Closing Date: Monday 11 September 2023
Salary: £37,099 per annum
Anticipated Interview Date: Wednesday 27 September 2023
Duration: Two fixed term positions available for 24 months and 30 months

JOB PURPOSE:

To conduct research into the application of advanced machine learning techniques for use semiconductor security and specifically in hardware Trojan detection. This project will be hosted by the Centre for Secure Information Technology at Queen's University Belfast and is associated with the Research Institute in Secure Hardware and Embedded Systems. Please note that all staff on the project are required to undergo Baseline Personnel Security Standard checks.

MAJOR DUTIES:

1. Conduct research into the application of trustworthy (secure and explainable) machine learning and deep learning techniques in Hardware Trojan detection and to collaboratively work on security verification in Electronic Design Automation (EDA) Tools.
2. Actively contribute to the general planning and delivery of the overall research project activities.
3. Present annual progress reports on research for funders and to the UK research community via RISE, to CSIT industry advisory board members or to external audiences to disseminate and publicise research findings.
4. Prepare, in consultation with supervisor, material for publication in national and international journals and presentations at international conferences.
5. Assist in the preparation of funding proposals and applications to external bodies.
6. Carry out routine administrative tasks associated with the research project. This might include organisation of project meetings and documentation, financial control, risk assessment of research activities.
7. Carry out occasional undergraduate/postgraduate student project supervision, demonstrating or lecturing duties within the post holder's area of expertise and under the direct guidance of a member of academic staff.
8. Read academic papers, journals and textbooks to keep abreast of developments in own specialism and related disciplines.
9. Any other duties that may reasonably be requested by the programme supervisor.

ESSENTIAL CRITERIA:

1. 2:1 Honours degree in Electrical and Electronic Engineering/Computer Science/Mathematics (or related discipline).
2. Have, or be about to obtain, a PhD in a relevant subject.
3. Relevant research experience in Machine Learning.
4. Evidence of a strong publication record commensurate with career stage and experience.
5. Demonstrable ability to contribute to broader management and administrative processes.
6. Demonstrable ability to contribute to the School's outreach programme by establishing links with industry, community groups etc.
7. Sufficient breadth and depth of specialist knowledge in the discipline and of research methods and techniques to work within established research programmes.
8. Good written and verbal communication skills.
9. Proven ability to communicate complex information clearly.
10. Demonstrable ability to innovate and rapidly contribute to research projects.
11. Willingness to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.

DESIRABLE CRITERIA:

1. Expertise in Adversarial ML or Explainable AI.
2. Expertise in hardware security, especially Hardware Trojan design and/or detection.
3. Ability to build contacts and participate in internal and external networks.
4. Experience of collaborative research or working in a team is desirable.