Candidate Information

Position:	Research Fellow (Hardware-aware AI Security)
School/Department:	School of Electronics, Electrical Engineering and Computer Science
Reference:	25/113039
Closing Date:	Monday 12 January 2026
Salary:	£41,519- £44,035 per annum
Anticipated Interview Date:	Thursday 22 January 2026
Duration:	Available until 31 December 2028

JOB PURPOSE:

The Chiplet-Guard project addresses the critical gap of AI Security in Chiplet context by developing a novel Trustworthy AI-based Global Security Monitoring (GSM) paradigm for holistic, interoperable security in chiplet systems. This 3-year EPSRC-funded research is conducted collaboratively between the University of Oxford and Queen's University Belfast's Centre for Secure Information Technologies (CSIT).

The Research Fellow will lead the development of AI-based security monitoring solutions capable of detecting advanced malware threats across heterogeneous Chiplet architectures, taking into account the inherent AI vulnerabilities. This role sits at the intersection of AI for security, AI security, hardware security, and computer architecture, contributing to a first-of-its-kind security framework for next-generation Hw/Sw computing systems that will have significant impact on the semiconductor industry and critical infrastructure security.

MAJOR DUTIES:

1. Undertake novel research on the security of edge AI systems with a focus on hardware vulnerabilities and the Chiplet context.
2. Design and develop machine learning models for security threat detection in complex, heterogeneous computing systems.
3. Investigate and model hardware attack surfaces including side-channel leakage, fault injection, and fault propagation.
4. Develop and evaluate mitigation strategies and trade-off models to balance security, performance, and energy efficiency.
5. Explore secure AI approaches for threat detection as well as different learning paradigms to address real-world constraints
6. Contribute to impactful publications and present research at major international venues in AI security and hardware-aware systems (e.g., IEEE S&P, USENIX, ISCA, MICRO, DAC, CHES, etc).
7. Engage with industrial partners and stakeholders to communicate research outcomes.
8. Contribute to project reports, deliverables, and documentation.
9. Participate in system integration activities, working across different technology platforms and simulation environments.
10. Collaborate with the wider project team, in both Queen’s and Oxford, and contribute to industry-facing dissemination activities.
11. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
12. Undertake supplementary duties relevant to the success of the project including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Normally have or about to obtain a PhD in computer science, engineering, mathematics or physical sciences area.
2. Significant relevant research experience in machine learning/AI, Embedded Systems or both, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Excellent analytical and problem-solving skills with ability to work on complex, multidisciplinary challenges.
4. Strong written and verbal communication skills, including ability to write high-quality research papers.
5. Strong motivation for conducting cutting-edge research in emerging security challenges.
6. Intellectual curiosity and enthusiasm for learning across disciplinary boundaries (AI, hardware, security).
7. Collaborative mindset with willingness to work across institutional boundaries (Oxford-QUB collaboration).

8. Commitment to research integrity and responsible innovation principles.
9. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
10. On-site presence required in accordance with QUB policy (currently for a minimum 3 days per week).

DESIRABLE CRITERIA:

1. PhD in hardware-aware AI security, computer architecture, or hardware security.
2. Experience with malware analysis, threat detection, or intrusion detection systems.
3. Knowledge of computer architecture concepts, particularly hardware performance monitoring (e.g., Hardware Performance Counters).
4. Experience in AI security and/or Trustworthy AI.
5. Understanding of Chiplet architectures and heterogeneous computing platforms (CPU-GPU systems, accelerators).
6. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc.)
7. Experience with Hardware design platforms.
8. Demonstrate resilience and the ability to work in a fast-changing environment with competing priorities.
9. Interest in mentoring junior researchers and students.
10. Ability to communicate complex technical concepts to diverse audiences including industry stakeholders.
11. Proactive approach to identifying new research opportunities and directions.