RISE
RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

QUEEN'S
UNIVERSITY
BELFAST

RISE ANNUAL REPORT

2023–2024

Funded by

in association with
National Cyber
Security Centre

EPSRC
Pioneering research
and skills

CONTENTS

FOREWORD

Since our last annual report, we have concluded the inaugural phase of funding for the Research Institute for Secure Hardware and Embedded Systems (RISE). Launched in 2017, RISE has worked towards establishing itself as a global hub for research and innovation in hardware security. The institute's strategic approach includes fostering close engagement with leading industry partners and stakeholders both within the UK and internationally, with a strong focus on translating research outcomes into practical products, services, and business opportunities to bolster the UK economy.

The National Cyber Security Centre (NCSC) — a part of GCHQ — has now approved funding for RISE Phase 2 from 2023–2026, which is hosted under Professor Máire O'Neill at the Centre for Secure Information Technologies (CSIT), within the School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast (QUB). Three new RISE-affiliated research projects have also been funded by the Engineering and Physical Sciences Research Council (EPSRC), bolstering hardware and embedded systems security research, innovation, and industry partnerships.

With the publication of the UK's National Semiconductor Strategy in May 2023, a key focus of which is to build on our hardware strengths to improve cyber security and ensure that *'cyber security is considered, and more widely prioritised, at the design stage of chips'*, RISE stands poised to contribute significantly, enhancing the UK's international research standing while augmenting economic competitiveness.

During RISE Phase 1 we made excellent progress across our funded research projects, we hosted a range of spring/summer schools and dedicated training course in hardware embedded systems security, we established an international partnership between the core RISE partners, namely QUB and the Universities of Bristol, Birmingham and Cambridge, and Nanyang Technological University (NTU) and National University of Singapore (NUS) and launched a UK competition targeting final year UG/MSc students, sponsored by ARM, to help stimulate the next generation of UK hardware security experts.

Significant research outputs to date include:

- Plundervolt — an attack developed as part of the University of Birmingham funded project which exploited vulnerabilities with Intel's Software Guard Extensions, leading to errors that could leak secret information such as encryption keys.
- Thunderclap — research by the University of Cambridge team that identified vulnerabilities with USB and Thunderbolt interface standards, and which provided security recommendations for hardening systems that were incorporated into the USB 4 standard.
- An Apple Pay vulnerability discovered by the University of Surrey's RISE project which showed that Apple Pay in Express Transit mode if used with a Visa card could be abused to make an Apple Pay payment to any shop terminal, of any value, without the need for user authentication.
- A Queen's University Belfast project led to the first deep-learning based automated Hardware Trojan (HT) detection system based on gate-level netlists to effectively detect HTs without any pre-knowledge of the circuits. HTs are malicious modifications of integrated circuits.
- A trusted FPGA environment developed by the University of Manchester team that solves two problems; firstly, it uses their FPGADefender virus scanner to help a cloud service provider (CSP) ensure a user bitstream is not malicious, and secondly, it ensures user IP protection by configuring an FPGA only with encrypted configuration bitstreams.

Phase 2 will involve annual RISE conferences; spring/summer schools; early career researcher training and innovation workshops; a UK/US Workshop on Semiconductor Security; and a UK-wide Training Roadshow. The aligned funding from EPSRC supports three new research projects addressing 'Trustworthy Deep-Learning based Hardware Trojan Detection' at Queen's University Belfast, 'Securing and Analysing Trusted Execution Beyond the CPU' at the Universities of Southampton and Birmingham, and 'Securing Composable Hardware Platforms' at the University of Manchester.

RISE will continue to play its part in conducting research that addresses security throughout a device's lifecycle, from the initial design and manufacture through to its operational environment. We will also continue to grow the skillsets and community in the UK in this strategically important area, and help to support the delivery of the security pillar of the National Semiconductor Strategy.

Professor Máire O'Neill, RISE Director
Queen's University Belfast

THE RESEARCH INSTITUTE FOR SECURE HARDWARE AND EMBEDDED SYSTEMS

The £5M Research Institute for Secure Hardware and Embedded Systems (RISE), which is hosted at the Centre for Secure Information Technologies (CSIT), Queen's University Belfast, seeks to identify and address key issues that underpin our understanding of Hardware Security. Funded by the Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC), RISE is one of four cyber security institutes in the UK and aims to be a global hub for research and innovation in hardware security.

RISE aims to address the following research challenges in Hardware Security:

1. **Understanding the technologies that underpin hardware security, the vulnerabilities in these technologies and development of countermeasures.**
    - State-of-the-art Hardware Security primitives: True Random Number Generators (TRNGs), Physical Unclonable Functions (PUFs).
    - Novel Hardware analysis toolsets and techniques.
    - Attack-resilient Hardware platforms, Hardware IP building blocks.

2. **Maintain confidence in security throughout the development process and product lifecycle.**
    - Confidence in Developing Secure Hardware devices.
    - Supply Chain Confidence.
    - Modelling of Hardware Security.

3. **Hardware security use cases and consideration of value propositions.**
    - Novel Authentication, e.g. alternatives to passwords.
    - Secure document viewers.
    - Securing BYOD – attestation, roots of trust.

4. **Development and pull through.**
    - Ease of Development and ease of leveraging best security options.
    - Understanding Barriers to Adoption.
    - Education of Potential User/Developer base.

THE RISE INSTITUTE MODEL

Fulfilling the aims of a global centre for research and innovation in hardware security requires not only world-class research, but also close engagement with leading UK-based industry partners and stakeholders. This additional focus facilitates the accelerated translation of research output into new products, services and business opportunities for the wider benefit of the UK economy.

The key elements within RISE are the academic researchers, an Industry & Stakeholder Advisory Board (ISAB) and the Institute Management team.

The RISE ISAB is chaired by Charles Brookson OBE, and has been created to allow member companies and stakeholders to engage with the research community and to inform funding calls around their real world challenges.

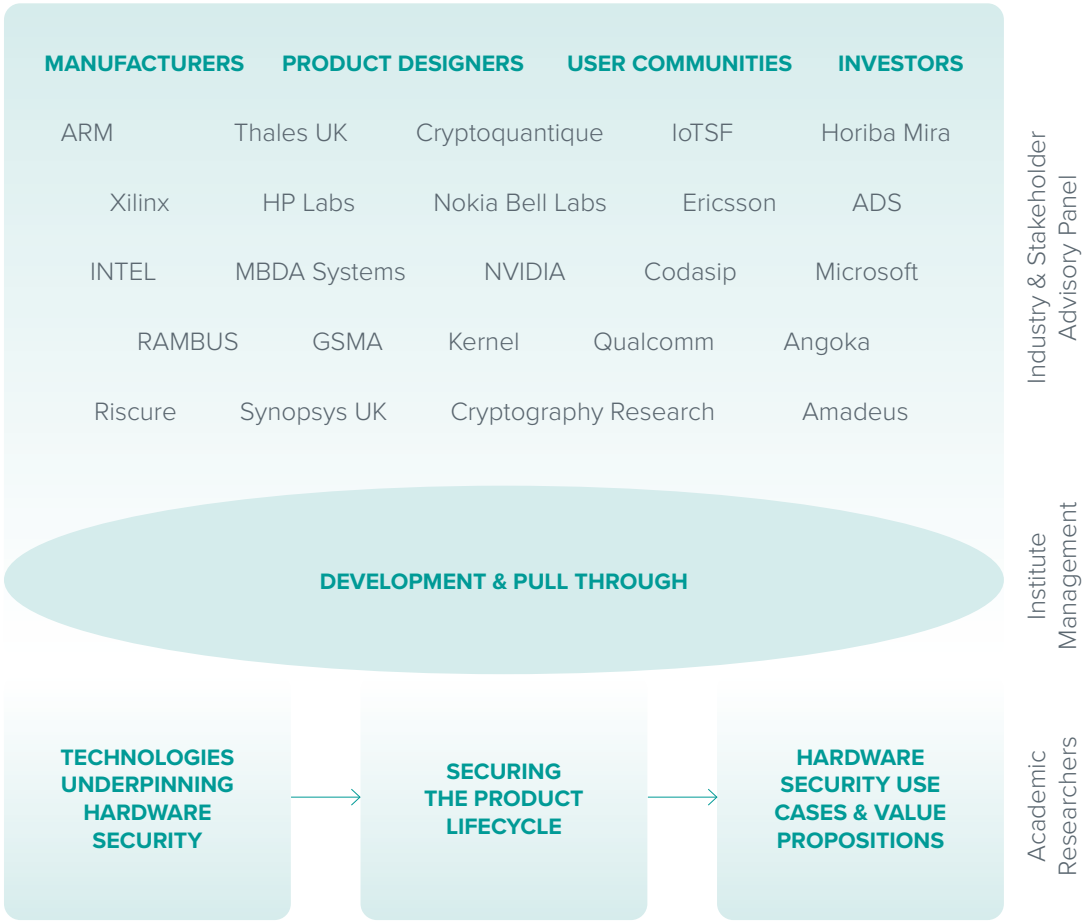
Other functions include:

- Receiving briefings on significant research outputs.
- Identification of research results, which are particularly appropriate for rapid commercialisation.
- Offer pathways to impact, e.g. licensing, spin-out support.
- Highlighting shifts in technology or market demand with significance for RISE.
- Informing future RISE research proposal calls.
- Helping to build a hardware security community in the UK.

The Institute Management team, incorporating leadership and business development, functions to drive forward the development and promotion of the institute to industry and other stakeholders.

You can find out more about RISE and its activities by visiting **www.ukrise.org**

RISE ECOSYSTEM



RISE AFFILIATED PROJECTS

The RISE research challenges are being delivered through a series of projects. Following an EPSRC funding call, three projects were successful in receiving grant awards, and will be delivered over the course of 2023–2026.

TRUDETECT: TRUSTWORTHY DEEP-LEARNING HARDWARE TROJAN DETECTION

Prof Máire O'Neill
Dr Ihsen Alouani
Dr Niall McLaughlin

The modern semiconductor supply chain uses overseas foundries, third-party IP and third-party test facilities. However, with so many different untrusted entities, this design and fabrication outsourcing has exposed silicon chips to a range of hardware-based security threats such as counterfeiting, IP piracy, reverse engineering and hardware Trojans (HT).

A hardware Trojan is a malicious modification of a circuit in order to control, modify, disable, monitor or affect the operation of the circuit. Although there have been no public reports of HTs detected in practice, in 2020, the cybersecurity company F-Secure published a report on their investigation into a pair of counterfeit Cisco Catalyst 2960-X series switches . While these devices did not have back-door functionality, they did employ measures to bypass processes that authenticate system components and F-Secure stated that motivated attackers use the same approach to insert hardware trojans to stealthily backdoor companies.

Such hardware threats are major security threats for safety-critical and embedded systems applications, e.g. in the medical, automotive or transport sectors. Due to the nature of this clandestine industry, it is very difficult to ascertain the true scale of the problem. However, in recent years both the sovereignty and cyber security of the semiconductor supply chain have become significant concerns for many countries.

The recently published EU Cyber Resilience Act (September 2022) outlines essential cybersecurity requirements for products with digital elements and states that such produced 'shall be delivered without any known exploitable vulnerabilities'. In addition, the 2022 National Cyber Strategy 2022 outlines the need to 'ensure that wherever possible the next generation of connected technologies are designed, developed, and deployed with security and resilience in mind and embrace a 'secure by design' approach'.

The overall goal of the TruDetect project is to develop a trustworthy DL-based HT detection system that can be easily integrated into a security verification framework in EDA tools. This will include the design of novel countermeasures that ensure trustworthiness of the DL-based HT detection system against adversarial HTs and the use of Explainable AI to offer a comprehensive analysis of the DL system behaviour.

IOTEE: SECURING AND ANALYSING TRUSTED EXECUTION BEYOND THE CPU

UNIVERSITY OF BIRMINGHAM

University of Southampton

Prof David Oswald
Prof Mark Ryan

Dr Ahmad Atamli
Prof Vladi Sassone

Trusted Execution Environments (TEEs) allow users to run their software in a secure enclave while assuring the integrity and confidentiality of data and applications. However, cloud computing these days relies heavily on peripherals such as GPUs, NICs, and FPGAs. Extending the security guarantees of CPU TEEs to such accelerators is currently not possible. New technologies are being proposed to address this, notably the PCIe Trusted Device Interface Security Protocol (TDISP).

IOTEE aims to evaluate the security guarantees of this new PCIe standard and its ability to provide trusted execution against strong adversaries. This will involve developing an emulator for the protocol, the use of formal modelling, as well as researching countermeasures against various software and hardware attacks.

SECCOM: SECURING COMPOSABLE HARDWARE PLATFORMS

The University of Manchester

Prof John Goodacre
Dr Bernardo Magri
Dr Lucas Cordeiro

This project seeks to identify and address the critical security issues arising from the creation of hardware platforms through the use of composable hardware systems.

Predominantly, current hardware architectures are statically defined and deliver therefore a predetermined level of security and properties by which its resilience can be verified.

In the simplest case, a static design supporting hardware extension, for example through an exported bus, such as PCIe, will deviate from the design's initial security principles and will require mechanisms of encapsulation in its security model to constrain the indeterminable mechanisms by which extension of a system can perturb a static security model.

Although the provision of composable hardware may have understood security principles covering the creation of the resulting hardware platform, the arbitrary nature of composing the elements of a computer means that the resulting permutations lack any model of security by which threat models and mitigations can be evaluated.

The project proposes to conceptualise and evaluate across the design space of composable hardware platforms to discover whether key security properties and threat models can be extracted and used to create a security model from which the security of composed hardware can be validated. Further, given the dynamic nature of composed hardware, we will also investigate whether composed hardware can use dynamic verification mechanisms to assert security policy at runtime.

Beginning with platforms composed using PCI express switches in which the devices of a host can be shared and allocated dynamically between hosts, we will investigate the evolving and increased flexibility from Compute Express Link (CXL) and its ability to remove the host and device hierarchy while permitting any compute element to be a host or device while also providing shared access across the platform.

The objective outcome is to provide industry with a security model for a composed hardware platform from which security principles can be reasoned and demonstrated by its dynamic verification.

UK-US SEMICONDUCTOR SECURITY WORKSHOP

RISE hosted a very successful UK/US Workshop on 'Security in the Era of Global Semiconductor Initiatives' on 28th/29th November in Washington DC, chaired by Professor Máire O'Neill and Prof. Mark M. Tehranipoor, University of Florida.

The workshop brought together leading UK and US industry, government, and academic experts in semiconductor security to discuss the challenges and opportunities in this sector. The themes of the workshop included:

- Hardware Security Primitives
- RISC-V security
- Semiconductor supply chain security
- Hardware-based attacks and countermeasures
- Formal methods and tools for secure design and verification
- System security

The conference included individual talks in addition to a panel discussion on "Is Secure-by-Design Hardware achievable?" and roundtable discussions on pre-silicon, post-silicon, system security and supply chain security.

Workshop Chairs

Prof Máire O'Neill, FREng
Regius Professor in Electronics and Computer Engineering, Director, Research Institute in Secure Hardware & Embedded Systems (RISE), Queens University Belfast, UK

Prof Mark M Tehranipoor
Intel Charles E Young Pre-eminences Endowed Chair Professor in Cybersecurity, Chair, Department of ECE, University of Florida, US

Workshop Contributors

Government Representatives

UK Department of Science, Innovation and Technology (DSIT)
UK Defence Science and Technology Laboratory (DSTL)
UK National Cyber Security Centre (NCSC)
US CHIPS Program Office
US Department of Homeland Security
US National Institute of Standards and Technology (NIST)
US Defense Advanced Research Projects Agency (DARPA)

Industry Representatives

Dan O'Loughlin, VP Engineering, Qualcomm
Adam Cron, Distinguished Architect, Synopsys
John Oakley, Semiconductor Research Corporation (SRC), US
Angela Dalton, Director, AMD Research & Advanced Development, AMD
Doug Gardner, Chief Technologist, Analog Devices
David Maidment, Arm
Shawn Fetterolf, Intel
Sid Allman, Senior Technical Director, Marvell Technologies
Manuel Offenberg, CTO/Chief Architect, Seagate Federal
Patrik Ekdahl, Manager Platform Security, Ericsson

Academic Representatives

John Goodenough, University of Sheffield
John Goodacre, University of Manchester
Simon Moore, University of Cambridge
Dan Page, University of Bristol
Ahmed Atamli, University of Southampton
Waleed Khalil, Ohio State University
Farinaz Koushanfar, University of California San Diego
Shreyas Sen, Purdue University
Aydin Aysu, North Carolina State University
Ramesh Karri, New York University
Gang Qu, University of Maryland
Farimah Farahmandi, University of Florida

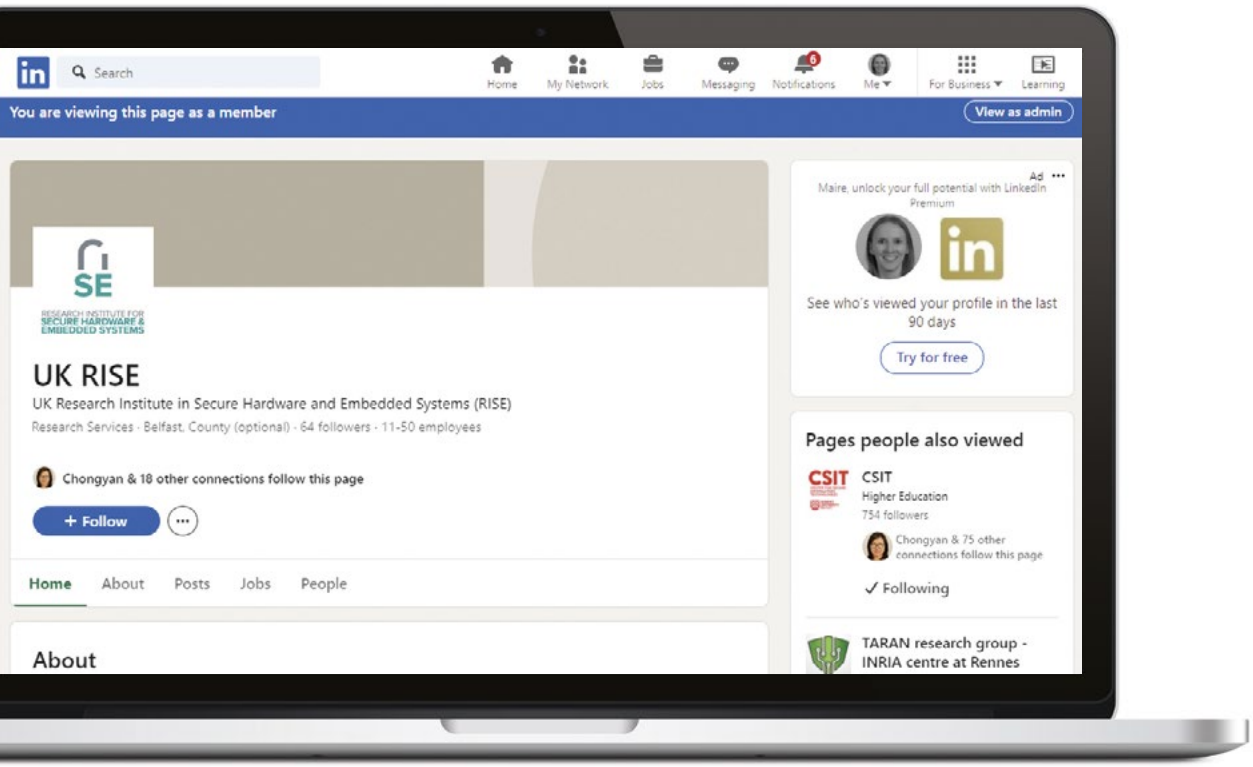
Opening Welcome by Saqib Bhatti MP MBE, UK Minister for Tech and the Digital Economy

Dr Farimah Farahmandi, University of Florida

John Oakley, Semiconductor Research Corporation

NEW RISE LINKEDIN PRESENCE

We launched a RISE Linkedin page to complement our X social media presence.



Social Media activity included our Phase 2 launch announcement, highlights from the UK-US semiconductor security workshop, and dissemination of the White House report recommending the use of CHERI technology from RISE core partner, the University of Cambridge.

Follow us for news, updates and information on upcoming events.

SECURITY IN THE ERA OF GLOBAL SEMICONDUCTOR INITIATIVES

CHALLENGES AND OPPORTUNITIES REPORT

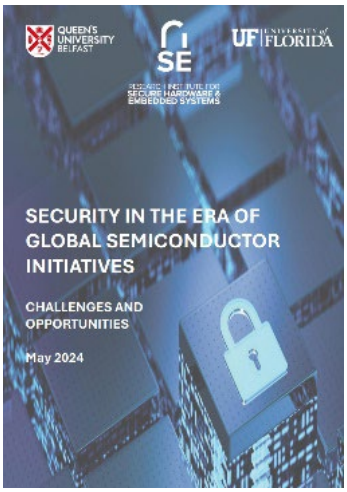
Spurred by the insights from the workshop on Security in the Era of Global Semiconductor Initiatives, a report has been published providing a strategic overview of the current challenges and emergent opportunities in semiconductor security.

The many significant security challenges confronting the semiconductor industry are considered, ranging from the complexity of semiconductor designs and the viability of secure-by-design methodologies, to securing the hardware design lifecycle and mitigating risks associated with chiplets and supply chain vulnerabilities. The report also discusses the threats posed by side-channel attacks and the critical skills shortage in hardware security.

On the opportunities front, the report highlights secure-by-design approaches as essential for building inherently secure systems from the ground up. It advocates for the creation of a hardware vulnerability database to catalogue known hardware vulnerabilities, enhancing supply chain security measures, and leveraging automation and artificial intelligence (AI) to manage design complexity and enhance security. The report also underscores the value of open-source hardware security IP in fostering innovation and security within the semiconductor industry, alongside the necessity for quantifiable assurance through metrics and standards to quantify security assurance of hardware components throughout their lifecycle. Enhanced training and collaboration among industry, academia, and government are emphasized as vital to sharing knowledge and best practices to address semiconductor security challenges effectively.

The key recommendations arising from the report are as follows:

1. Provide Support for Secure-by-Design Initiatives
2. Balance Security with Performance
3. Create a Hardware Vulnerability Database
4. Adopt Security Mechanisms offering Traceability and Provenance
5. Research and Develop AI Enhanced Semiconductor Security Design
6. Adopt Open-Source Hardware
7. Establish Industry Standards and Metrics
8. Invest in Education and Training
9. Invest in Collaborative Research and Development



The report can be found on the RISE website at
www.ukrise.org/semiconductor-secuirty-report.pdf

NCSC PROBLEM BOOK

RISE helped inform NCSC's research problem book.

The key problems identified include:

1. **How do our devices physically behave, and how do we secure those behaviours?**
   To address physical attacks, and to establish the behaviour on which the rest of the system builds.

2. **How do we know that we can trust our devices?**
   It's important to understand the amount of trust we have in a device, and the limits of that trust.

3. **What device architectures help us to improve security further up the stack?**
   To build devices that meet our security goals by design.

4. **How do we integrate secure devices, to ensure that the security still holds at the system level?**
   To make it easy to build a secure system without needing to be an expert in every device used.

The problem book provides details to justify the identified problems, outlining why each is important. The full problem book can be found at the following link:

www.ncsc.gov.uk/collection/problem-book

How do our devices physically behave, and how do we monitor and secure those behaviours?

Why this is important

It's not currently feasible to gain confidence that a device you haven't designed and manufactured yourself doesn't contain anything malicious, and meets your own standards of testing and verification. This means that a product manufacturer can't truly trust in the devices they include in their systems. But if we can improve our understanding and demonstrate the security and trust you get from any given device, we can begin to mitigate supply chain risks. This directly feeds into how we build trusted and resilient systems, for both commodity and high-assurance uses.

Máire O'Neill, Professor of Information Security, Queen's University Belfast.

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

CONTACT DETAILS
W: www.ukrise.org
E: info@ukrise.org.uk
T: +44 (0) 28 9097 1771
@UK_RISE