UNIVERSITY OF SURREY

SURREY CENTRE FOR CYBER SECURITY

Surrey Centre for SCCS Cyber Security

CONTENTS

WELCOME

to the Surrey Centre for Cyber Security

Professor Steve Schneider

S Schneider

Professor Ioana Boureanu

Security and privacy in the modern digital world is truly a myriad of topics in informatics, in technology and social sciences: from the mathematical foundations of cryptography all the way to the psychology and sociology of human factors.

Research in this field is therefore spanning the breadth and depth of blue-sky endeavours all the way to applied and industrial research as well as market-ready outputs.

Surrey Centre for Cyber Security (SCCS) - an Academic Centre of Excellence in Cyber Security Research - focuses on technical foundations of cyber security and privacy and their applications, to mitigate the threats faced by individuals and organisations.

We collaborate closely with industry and government, as well as other academic institutions, to build security into emerging and future technologies. We have an excellent track record of winning competitive bids with our partners, securing funding from bodies such as EPSRC (Engineering and Physical Sciences Research Council), EU Horizon 2020, EIT Digital and Innovate UK. We also offer joint studentships with EPSRC and organise placements for our masters and undergraduate students within relevant industrial companies.

Our areas of expertise include trusted systems, formal modelling & verification, distributed systems, blockchain & distributed ledger technologies, communication & networks, social media, and applied cryptography. Using these technologies, we strive to develop solutions that will enable society and industry to benefit from advanced technology in a secure way.

Surrey Centre for Cyber Security

Surrey Centre for Cyber Security (SCCS) consolidates research activities in cyber security across the University of Surrey. Based in the Department of Computer Science, the Centre collaborates with experts from Electrical and Electronic Engineering, Sociology, Psychology, Business, Law and Economics.

SCCS also provides a platform to explore the cyber security challenges being presented by next-generation mobile communications via joint research with Surrey's 5G Innovation Centre (5GIC) – the UK's largest academic research centre dedicated to developing next generation mobile and wireless communications.

Academic Centre of Excellence in Cyber Security Research and Education

The University of Surrey is one of only six universities in the UK to be recognised by the government's National Cyber Security Centre (NCSC) as both an Academic Centre of Excellence in Cyber Security Research (ACE-CSR) and Academic Centre of Excellence in Cyber Security Education (ACE-CSE). SCCS has had ACE-CSR status since 2015, while the University was given ACE-CSE recognition in 2020.

Gold Award

in association with
National Cyber
Security Centre

Department for
Digital, Culture,
Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

UK RI
Engineering and
Physical Sciences
Research Council

Academic Centre of
Excellence
in Cyber Security Research

ACE-CSR
in association with
National Cyber
Security Centre

ACADEMIC CENTRE OF EXCELLENCE IN CYBER SECURITY EDUCATION

Surrey is one of NCSC's Gold-level Academic Centre of Excellence in Cyber-Security Education (ACE-CSE). This is an accolade awarded to only ten universities in the UK.

A Pan-university, Virtual Institute. Our ACE-CSE is a pan-university, virtual institute, involving the SCCS members, other computer scientists, psychologists, sociologists, the IT department of the University including our Chief Security Officer (CISO); this is a growing team of facilitators in the different facets of cybersecurity and its education. We work together to provide fine-tuned cybersecurity education, training and awareness to our students, staff and the general public, as well as specific segments thereof.

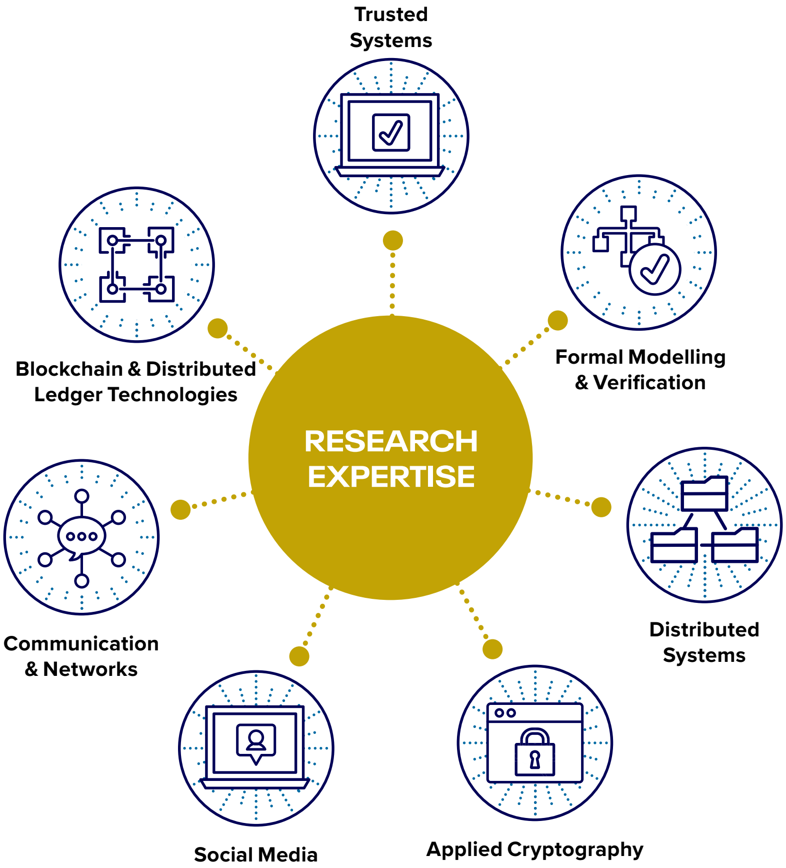
Wide Outreach in Cybersecurity Education. As an ACE-CSE, not only do we provide outstanding cybersecurity education to our STEM (science, technology, engineering, and mathematics) students, but we also provide significant cybersecurity training to social science and humanities students. Moreover, we run programmes of cybersecurity training for all our staff, including a proportion of them being instructed in accordance with the ISO27001 standard and in compliance with Cyber Essentials Plus and achieving cyber-security certifications. Finally, we are engaged with industry, charities, and local government, as well as general public, on matters of cybersecurity education: we organise seminar series, workshops, summer/winter postgraduate schools, present at science festivals, and take-in A/GCSE-level summer interns. As a case in point in 2022 and 2023, Surrey was the host of NCSC's CyberFirst initiative – whereby A-level pupils follow a residential, one-week course in cybersecurity.

Projects on Cybersecurity-Education. We also undertake research projects in pedagogic aspects of cybersecurity education and matters related to it. We exemplify two of these below.

Phish and Tips -- Cyber Security Outreach for Older Adults, PI Prof. Helen Treharne, Dr Dan Gardham (SCCS, Surrey), Dr Suzanne Prior (Abertay University), Dr Chris Culnane (Castellate Consulting Ltd.), October 2022-March 2023. This project complements guides being offered by charities supporting older members of our community and bringing phishing scam training to life through practical evaluation of emails. The aim of the project is to teach users how to develop appropriate risk analysis strategies when they receive emails, to allow them to better identify potential phishing emails and then act accordingly. The design philosophy is to develop a safe interactive training environment in which older people can build their confidence. Following feedback from our collaborating partners from UK charities, it is important that the training is not a gamification environment. Phish and Tips also uses focus groups of older adults across the UK, before and after interacting with the training environment. *Phish and Tips* is a follow-on to a previously funded project, *Practice Using Passwords*, which provided basic training on what are passwords, how to use security codes and CAPTCHA. Both projects sit alongside each other to deliver a holistic set of training support for the older community.

Train-CyRi -- Gamified Training on Cyber Risk with Assessment of Cybersecurity Awareness and Psychological Fears, co-PIs Dr Oliver Mason (Dept. of Psychology) & Prof. Ioana Boureanu (SCCS), October 2022- March 2023. Train-CyRi focuses on educational and psychological metrics related to cybersecurity education and cybersecurity fears. Given the uptake in using gamified cyber-education, in initiatives like CyberAware and programmes like CyberFirst, Train-CyRi aims to demonstrate both the acceptability of gamified cybersecurity training, as well as its educational value for individuals who are not exposed to cybersecurity, in turn leading to behaviour change across a significant proportion of those trained. Concretely, Train-CyRi consists of a study of perception of cyber fears on circa 50 non-STEM, cybersecurity-uneducated undergraduate students, before and after interacting with a gamified, training environment. The latter is developed within the UK Government's National Cyber Security Programme. Following on from Train-CyRi, we already partnered with Cyber Security Challenge UK (CSCUK) for a longer-term and wider study on educational and psychometrics of gamified cybersecurity training.

For further information, please write to us at ace-cse@surrey.ac.uk



RESEARCH EXPERTISE

Trusted Systems

Formal Modelling & Verification

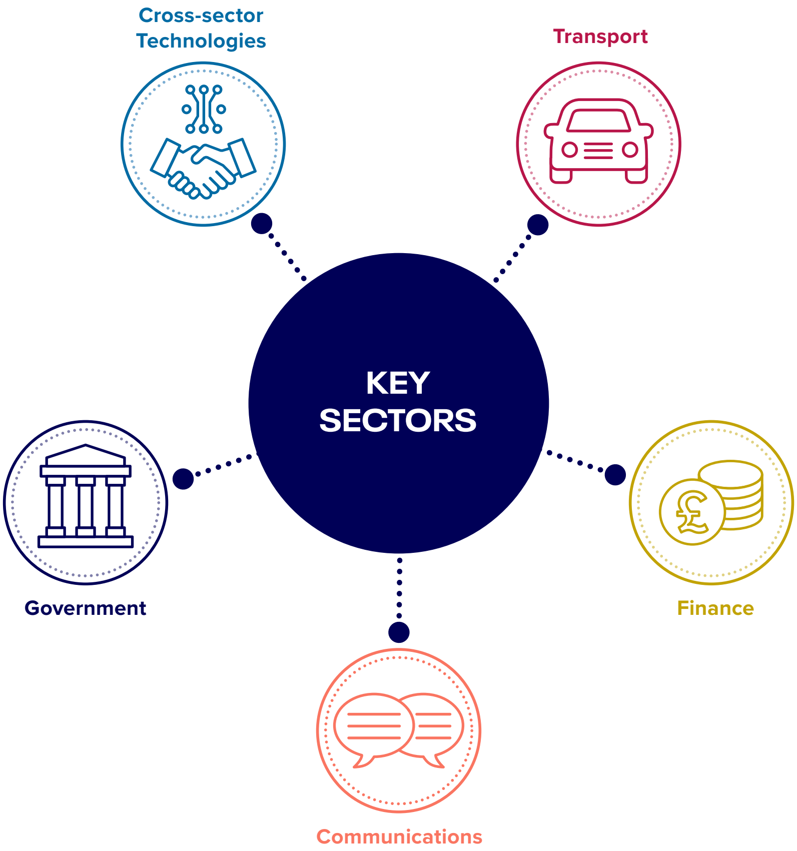
Distributed Systems

Applied Cryptography

Social Media

Communication & Networks

Blockchain & Distributed Ledger Technologies



KEY SECTORS

Cross-sector Technologies

Transport

Finance

Communications

Government

17

Academic Members

32

Researchers

£12m

Funding (since 2016)

40

Projects (since 2016)

1 of 6

UK universities recognised by NCSC for both research & education

NCSC Certified

Masters course in Information Security

SCCS TEAM

Professor Steve Schneider

Director of SCCS, Professor in Secure Systems

Research interests: e-voting, verification, security protocols, distributed ledger technology, trust, privacy, formal modelling.

Professor Ioana Boureanu

Deputy Director of SCCS,
Professor in Secure Systems

Research interests: provable security, automatic verification, authentication, key-exchange, formal methods for security/privacy.

Dr Rizwan Asghar

Associate Professor in Secure Systems
Research interests: Digital privacy, Cyber resilience, Cybersecurity education

Professor Liqun Chen

Professor in Secure Systems

Research interests: cryptography, trusted computing, hardware security.

Professor Gregory Chockler

Co-Head of Distributed and Networked Systems group

Research interests: secure and trustworthy distributed computing, fault-tolerant distributed algorithms, secure data replication and transaction processing, blockchain consensus.

Dr Suparna De

Lecturer in Computer Science

Research interests: Cyber-Physical-Social systems; Semantic search and modelling; Big Data analysis; Machine learning applications.

Dr Brijesh Dongol

Associate Professor in Secure Systems

Research interests: verification, distributed and concurrent systems, real-time and hybrid systems, autonomous systems, weak memory, algebra.

Dr Constantin Cătălin Drăgan

Lecturer in Secure Systems

Research interests: electronic voting, applied cryptography, provable security, formal verification, privacy-preserving technology.

Dr Daniel Gardham

Lecturer in Secure Systems

Research interests: applied cryptography, specifically privacy-preserving cryptography and authentication protocols.

Dr Lee Gillam

Associate Professor

Research interests: cloud and edge computing, connected and autonomous vehicles, cybercrime and online safety.

Dr Robert Granger

Senior Lecturer in Secure Systems

Research interests: computational number theory and algebraic geometry; their applications to cryptography and cryptanalysis; and finite fields.

Dr Sasa Radomirovic

Senior Lecturer in Secure Systems

Research interests: Formal Methods for Information Security; Formal Modelling and Verification of Cryptographic Protocols.

Professor Nishanth Sastry

Co-Head of Distributed and Networked Systems group

Research interests: online harms, web tracking and privacy, GDPR and web consent, internet data science and large-scale/in-the-wild measurements, edge networks, including applications of block chains.

Dr Jack Tian

Lecturer in Cyber Security

Research interests: applied cryptography, network security, blockchain technologies, privacy-preserving technologies.

Dr Ehsan Toreini

Lecturer in Secure Systems

Research interests: trustworthy machine learning, socio-technical impacts of web tracking, side channel attacks to sensors and other hardware components and web-based malware attacks and mitigations.

Professor Helen Treharne

Professor in Secure Systems

Research interests: formal verification, security verification, authentication, trusted computing, IoT applications, rail applications, intelligent mobility, useable security.

Professor Alan Woodward

Visiting Professor

Research interests: cryptography, steganography, watermarking and general computer security.

TRUSTED SYSTEMS

WE CAN USE HARDWARE TO MAKE SYSTEMS MORE SECURE; HOWEVER ADDING EXTRA HARDWARE IS COSTLY AND CAN MAKE THE SYSTEM INFLEXIBLE.

SINCE SECURITY IS AN EVOLVING PROBLEM – WHERE ATTACKERS COMPETE TO FIND FLAWS AND VULNERABILITIES IN DEFENSIVE MECHANISMS – INFLEXIBILITY CAN BE A REAL ISSUE. IN SCCS WE ARE WORKING TO DESIGN SECURITY MECHANISMS THAT PROVIDE SOME FLEXIBILITY AND CAN STILL BE CHEAPLY IMPLEMENTED IN HARDWARE.

FutureTPM

(Future proofing the connected world: a quantum-resistant trusted platform module)

Under the technical lead of the University of Surrey, a consortium of 15 academic and industry partners from across Europe have succeeded in creating a Quantum-Resistant (QR) Trusted Platform Module (TPM) – a hardware chip which is used as a 'root of trust' for a computing system. The QR crypto algorithms selected or developed by the consortium can be used in a new generation of TPM-based solutions to enable security when quantum computers become reality. These algorithms have been successfully demonstrated in sectors where privacy and security are crucial: online banking, activity tracking in healthcare, and device management.

Collaborating with the Trusted Computing Group (TCG), the consortium will now work on including the QR crypto algorithms – once standardised – into the next generation of TPM.

- **Budget:** €5m
- **Funding:** EU H2020
- **Centre lead:** Professor Liqun Chen
- **Partners:** TECHNIKON, UBITECH, IBM Research, Infineon Technologies, Suite5 Data Intelligence Solutions, INESC-ID, Huawei Technologies, VIVA Payment Services SA, Royal Holloway, University of London, University of Birmingham, Universite du Luxembourg, University of Piraeus Research Center, Technical University of Denmark
- **Timeframe:** 2018-2021

Find out more about FutureTPM: futurepm.eu

ASSURED

(Future Proofing of ICT Trust Chains: Sustainable Operational Assurance and Verification Remote Guards for Systems-of-Systems Security and Privacy)

In the ASSURED project, SCCS is working with 13 partners from nine countries to help shape the future development of secure and trustworthy Cyber-physical System of Systems (CPSoS) and services that can greatly benefit the lifecycle of various safety-critical application domains. The core objective is to leverage and enhance runtime property-based attestation and verification techniques in order to allow intelligent (unverified) controllers to perform within a predetermined envelope of acceptable behaviour. The solution developed will be demonstrated in four scenarios: smart manufacturing, smart cities, smart aerospace and smart satellite.

- **Funding:** EU Horizon 2020
- **Centre lead:** Professor Liqun Chen
- **Partners:** Martel Innovate, Mellanox Technologies, Intrasoft International, Uni Systems, Ubitech, Suite5, United Technologies Research Centre, Space, BIBA, DAEM S.A., DTU, Eindhoven University of Technology, Technische Universitat Darmstadt, TU Delft
- **Timeframe:** 2020-2023

Find out more about ASSURED: project-assured.eu

CONNECT

(Continuous and Efficient Cooperative Trust Management for Resilient CCAM)

This project aims to address the convergence of security and safety in Connected, Cooperative and Automated Mobility (CCAM) by assessing dynamic trust relationships and defining a trust reasoning framework based on which involved entities can establish trust for cooperatively executing safety-critical functions. Trusted Execution Environment (TEEs) will be essential to establishing a verifiable chain of trust throughout the entire application stack of the host vehicle, as well as protecting data in transit, at rest and in use. This is a HORIZON EUROPE project with the total grant amount of €5,996,019 and involves 17 partners from 9 countries and Surrey is the only UK partner.

Surrey will be responsible for designing and implement remote, runtime behaviour attestation services covering all phases of system’s execution, developing a secure and efficient communication between CCAM actors using Verifiable Credentials, and developing a certifiable way of monitoring the trustworthiness state of all CCAM nodes as well as performing software configuration updates in a secure an authentic way.

- **Budget:** £292,475 (or €339,375)
- **Funding:** Innovate UK (HORIZON EUROPE Guarantee Funding)
- **Centre lead:** Professor Liqun Chen
- **Co-Investigator:** Constantin Cătălin Drăgan
- **Partners:** TECHNIKON (AT), UBITECH (EL), Huawei Technologies (DE), Institute of Communication and Computer Systems (EL), ULM University (DE), Red Hat (IL), TRIALOG (FR), Denso Automotive (DE), INTEL Deutschland (DE), SUITES5 Data Intelligence Solutions (CY), UNISYSTEMS (EL), University of Twente (NL), FSCOM (FR), Politechnico di Torino (IT), IRT System X (FR).
- **Timeframe:** September 2022 – September 2025

SECANT

(Security and privacy protection in Internet of Things devices)

The SECANT project aims to deliver a holistic framework for cyber security risk assessment in order to enhance the digital security, privacy and personal data protection in complex Information and Communication Technology (ICT) infrastructures. During the project, a toolkit and platform will be developed, and demonstrated and validated.

- **Funding:** EU Horizon 2020
- **Centre lead:** Professor Liqun Chen
- **Partners:** European partners from industry and academia, coordinated by Everis Spain SL
- **Timeframe:** 2021-2024

REWIRE

(REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems Lifecycle)

This project aims to provide a framework for continuous security assessment of open-source and open-specification hardware and software for IoT devices and the development of cybersecurity certification in accordance with the requirements and guidelines of recent EU regulation Cyber security Act3. This will be achieved by designing safeguards for the entire workflow of secure processing; from Deployment and Operations of software-based System-of-Systems to their patch management to their patch management when new exploits have been identified during run-time, by providing new trust management mechanisms towards the auditability and certification of software and hardware open-source specifications. This is a HORIZON EUROPE project with the total grant amount of €4,489,161 and involves 13 partners from 10 countries and Surrey is the only UK partner.

Surrey will be responsible for designing attestation models and mechanisms for guaranteeing the operational integrity of the mission-critical operations of the deployments, establishing continuous authentication and authorization of devices to facilitate secure communication and data sharing, and implementing cryptographic primitives for enabling decentralised data integrity, secure access control and data sharing.

- **Budget:** £284,567 (or €330,200)
- **Funding:** Innovate UK (HORIZON EUROPE Guarantee Funding)
- **Centre lead:** Professor Liqun Chen
- **Co-Investigator:** Constantin Cătălin Drăgan
- **Partners:** UBITECH (EL), Université Catholique de Louvain (BE), Secura (NL), Nec Laboratories Europe (DE), Delft University of Technology (NL), SUITES5 Data Intelligence Solutions (CY), UNISYSTEMS (EL), 8 Bells (CY), Libre Space Foundation (EL), Kenotom (EL), Odin Solutions (ES), Collins Aerospace Ireland (IE), Advanced Laboratory on Embedded Systems (IT)
- **Timeframe:** October 2022 – October 2025

TimeTrust

(Robust timing via hardware roots of trust and non-standard hardware)

Led by SCCS, the TimeTrust project is using hardware roots of trust, such as tamper-resistant cryptographic chips, to build cyber systems which are better equipped against vulnerabilities related to distance and timing measurements. The main use-case of this project is that of contactless payments, to counter illicit payments that can be made from a distance even if touch-and-pay is supposed to disallow it. The project is looking both at the formal treatment of security (eg. mathematical proofs) and at practical aspects.

As part of this project, we published notable results in the area of contactless payments. Most notably, we influenced the payments industry via an attack we exhibited leading to any-value fraudulent payments in ApplePay and Visa systems. Moreover, one of the solution we proposed to remedy the underlying problem is now in the process of being integrated into the ISO/IEC 14443 standard for contactless environments.

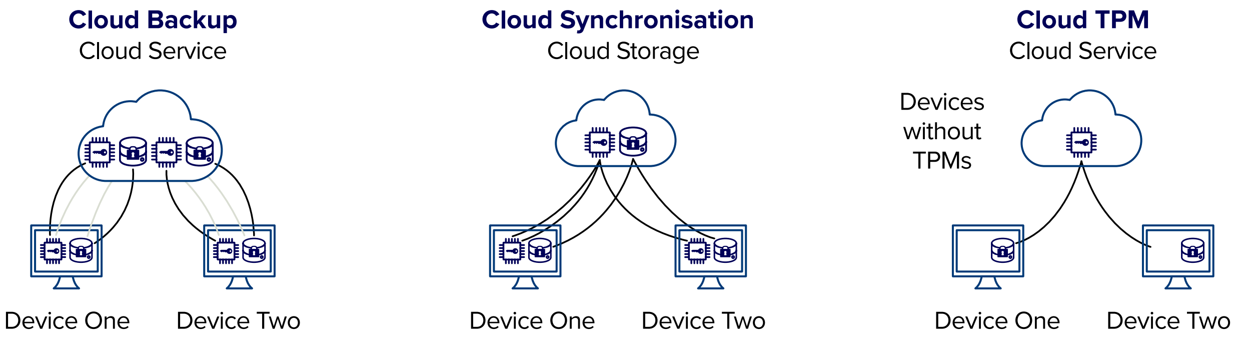
- **Budget:** £300,000
- **Funding:** EPSRC & NCSC under UK RISE
- **Centre lead:** Professor Ioana Boureanu
- **Partners:** Visa, Mastercard, Consult Hyperion, HP Labs, University of Birmingham
- **Timeframe:** April 2019 to November 2022

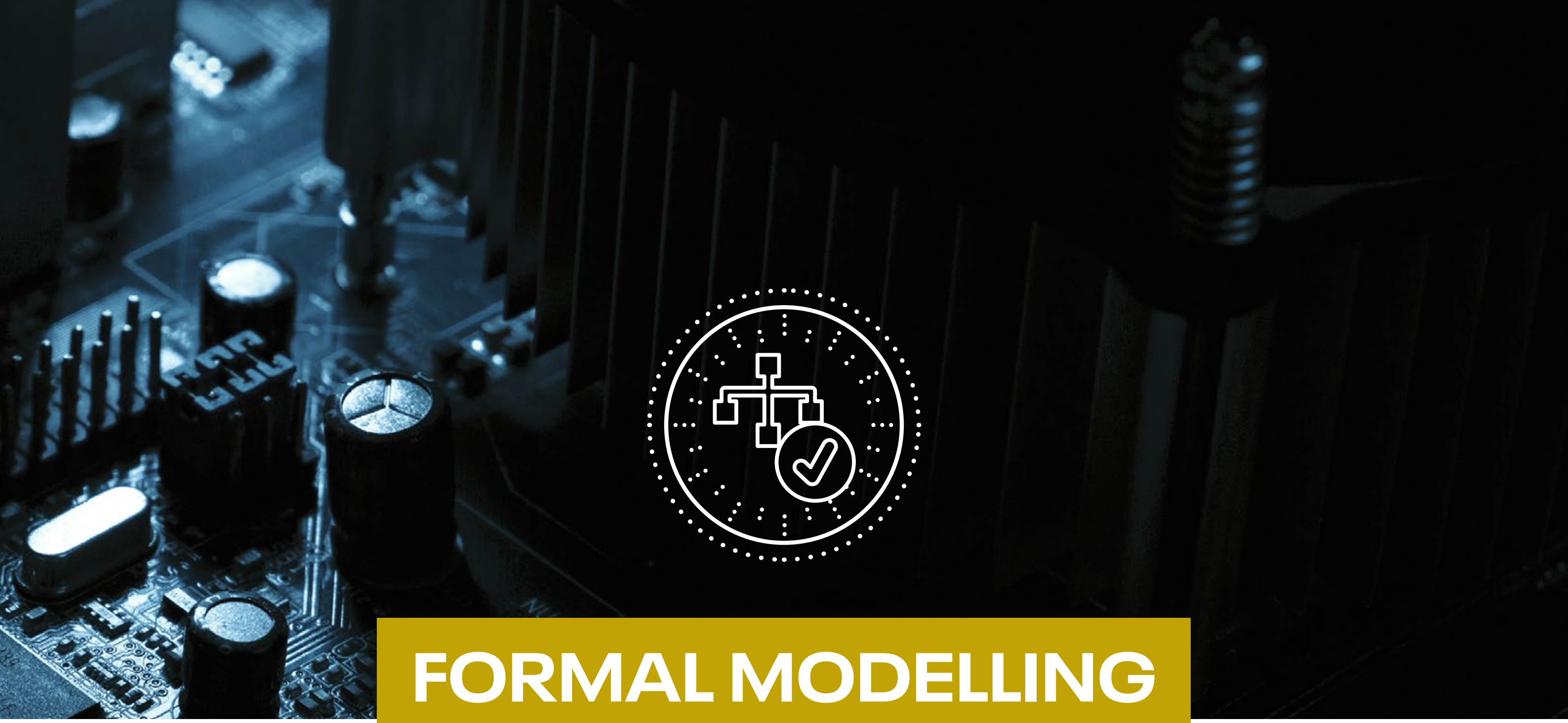
Scalable Passwordless Authentication Technologies

The focus of our research is to explore the security of passwordless architectures and how improve their resilience in the context of moving between devices. Importantly, also we are exploring the impact of human behaviour.

We have already developed a number of open source platforms which include a virtual WebAuthn authenticator in order to provide an extensible open source platform for understanding the associated standards of WebAuthn and CTAP2. By implementing a prototyping platform we are able to evaluate the underlying protocols in their current and future forms independent of the underlying hardware. Our authenticator also provides an alternative to an external physical hardware key and supports the use of a trusted platform module (TPM) on a device to generate the security keys within a WebAuthn protocol. Our open source platforms also include a cloud component to provide increased support when devices are lost or stolen.

- **Centre lead:** Professor Helen Treharne
- **Partners:** Castellate Consulting Ltd., Google
- **Timeframe:** 2021-2025





FORMAL MODELLING & VERIFICATION

SECURITY VERIFICATION – OBTAINING MATHEMATICAL PROOF OF THE BEHAVIOUR OF SYSTEMS AND PIECES OF HARDWARE – IS EMBEDDED INTO MANY OF OUR PROJECTS, ENSURING THAT FORMAL GUARANTEES ARE BUILT INTO EMERGING TECHNOLOGIES. AT SCCS OUR RESEARCHERS ARE EXPERTS IN 'CORRECTNESS', 'LIVENESS' (ENSURING THAT THE TECHNOLOGY IS ALWAYS READY TO TAKE THE NEXT STEP) AND VERIFICATION OF SECURITY PROPERTIES (ENSURING THAT THE SYSTEM IS NOT BEHAVING IN AN INSECURE WAY).

AutoPaSS

(Automatic verification of complex privacy requirements in unbounded-size secure systems)

With the advent of 5G and the Internet of Things, today's secure systems span an arbitrary number of executions and raise new privacy concerns. We therefore need new verification techniques that can capture these systems' unbounded sizes and ensure their privacy. To deliver the step-change needed in privacy analysis, the AutoPaSS project will create new algorithms and tools for privacy verification using AI-inspired formalisations. These formalisations express what we believe and what we know over the course of a given timeline, and this information can be used to model privacy (or lack of it) as well as formally verifying its presence or absence in an IT system.

This project is complemented by a foundational research project being undertaken by SCCS in collaboration with the Institute of Mathematical Sciences in Chennai, India, funded by the Royal Society.

As part of this project, we have yielded various theoretical developments, included a new automatic tool for the formal verification of privacy using AI-inspired logics. Importantly, we also exhibited privacy shortcomings onto LoRA IoT devices, and the LoRaWAN specification v 1.2 will include one of our proposed solutions for privacy provision in LoRaWAN.

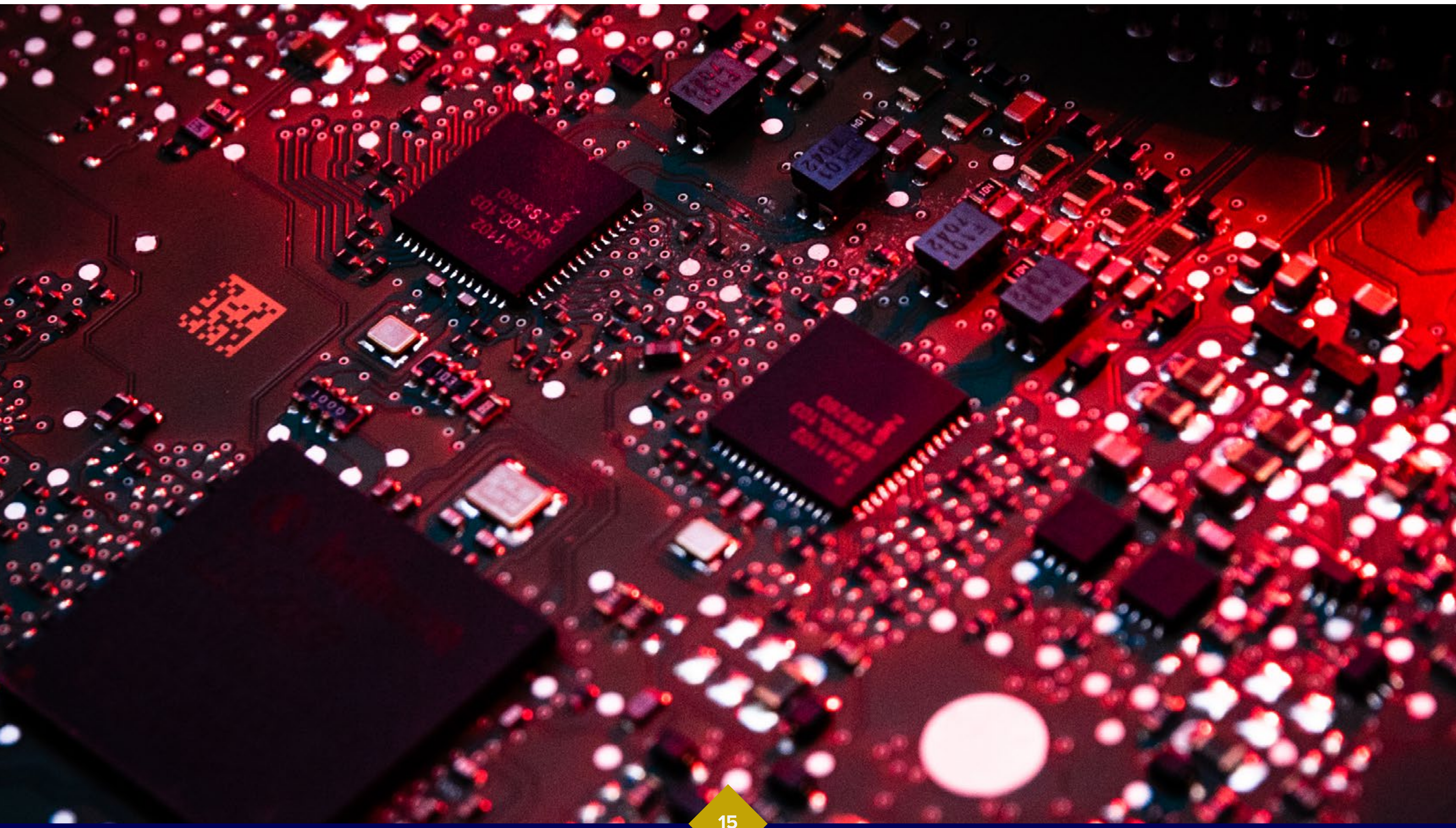
- **Budget:** £300,000
- **Funding:** EPSRC
- **Centre lead:** Professor Ioana Boureanu
- **Partners:** Thales Ltd, Vector
- **Timeframe:** July 2019 to November 2023

Verifiably Correct Swarm Attestation

This project is concerned with the use of attestation services, which provide a mechanism for establishing a trust relationship between a verifier and prover. Attestation is used where devices are required to authenticate their identity, ensuring the integrity and trust of the system software, and certifying that they are running a trusted code base.

We are interested in remote attestation, where a verifier checks the internal state of a prover on a different machine across a network, and in particular with swarm attestation services designed to attest a large number of medium/low-end devices. Our work considers formal verification of top-level swarm attestation protocols, and we use a correct-by-construction methodology to develop executable implementations. Then simulation will be used to show applicability of the swarm attestation protocols across real-world applications, including a vehicular simulation involving intelligent transport systems and an industrial control system developed in collaboration with our project partners.

- **Budget:** £514,155
- **Funding:** EPSRC
- **Centre lead:** Dr Brijesh Dongol
- **Co-Investigators:** Professor Liqun Chen, Professor Helen Treharne
- **Partners:** University of Sheffield, University of Kent
- **Associate Partners:** ARM Ltd, Nanyang Technological University, SRI International Inc, Thales Ltd
- **Timeframe:** 2021-2024



DISTRIBUTED SYSTEMS

IN DISTRIBUTED SYSTEMS, WHERE MULTIPLE AGENTS NEED TO TALK TO EACH OTHER TO ACCOMPLISH A TASK, ENSURING RESILIENCE TO FAILURE IS KEY TO PROVIDING AN UNINTERRUPTED SERVICE. BLOCKCHAIN HAS INTENSIFIED THIS CHALLENGE, WITH MALICIOUS BEHAVIOUR POTENTIALLY HAVING DEVASTATING EFFECTS – SUCH AS INVALIDATING THOUSANDS OF PAYMENT TRANSACTIONS. SCCS IS WORKING TO DEVELOP ALGORITHMS AND PROTOCOLS WHICH CAN PROVIDE CONTINUOUS SEPARATION AND ENABLE SYSTEMS WHICH ARE SCALABLE AND SECURE.

Stellar Payment Network

SCCS is working with Stellar Development Foundation to improve its open-source payment system. Running on blockchain, Stellar enables individuals and companies to create, send and trade digital representations of all forms of money (dollars, pesos, bitcoin etc), with the aim of allowing the world's financial systems to work together on a single network. In this project, SCCS will redesign several parts of the Stellar Consensus protocol, helping to solve potential problems with correctness and enabling the Stellar payment network to scale up to thousands of servers.

- **Budget:** $140,000
- **Funding:** Initially one year, subject to extension
- **Centre lead:** Professor Gregory Chockler
- **Partners:** IMDEA Software Institute (Madrid, Spain), Galois Inc (USA)
- **Timeframe:** 1 May 2021 – 1 May 2026

Find out more about Stellar Payment Network: stellar.org

LEADING INVENTOR OF DISTRIBUTED SYSTEMS TECHNOLOGY

Before moving into academia, **Professor Gregory Chockler** spent seven years as a researcher at IBM Research where he co-invented a new event-monitoring technology which boosted scalability of IBM's WebSphere Virtual Enterprise (among other products) by several orders of magnitude. He also co-invented Speculative Paxos, an award-winning reconfigurable replication protocol used in IBM cloud offerings to improve their availability and failure resilience.

Professor Chockler's current research focuses on blockchain and scalable information diffusion, with ongoing and recent projects funded by IBM and Facebook.

BLOCKCHAIN & DISTRIBUTED LEDGER TECHNOLOGIES

BLOCKCHAIN ENABLES US TO KEEP TAMPER-PROOF DATA WITHOUT RELYING ON A CENTRALISED AUTHORITY. TOGETHER WITH SURREY'S CENTRE FOR VISION, SPEECH AND SIGNAL PROCESSING AND THE CENTRE OF DIGITAL ECONOMY, SCCS IS LEADING THE WAY IN DISTRIBUTED LEDGER TECHNOLOGY (DLT) RESEARCH FOR THE PUBLIC GOOD, WITH A BROAD PORTFOLIO OF PROJECTS TO ENABLE GREATER TRUST ONLINE.

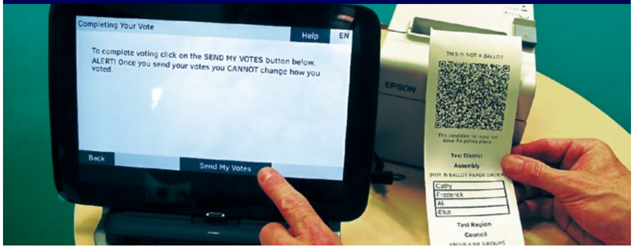
VOLT

(Voting On Ledger Technologies)

The fact that many elections are still run using paper ballots demonstrates that, despite the convenience and efficiency of electronic elections, there are unresolved security challenges around voting systems that could be vulnerable to malicious attack. The VOLT project explores the use of DLTs to enhance trust in electronic voting by providing transparency and an agreed tamperproof record of the election. The project is developing and piloting end-to-end verifiability into online voting, and also applying smart contracts to the management of voting rights for shareholders in the corporate environment – particularly for crowdfunded businesses.

- **Find out more about VOLT:** blockchain.surrey.ac.uk/projects/volt.html

- **Budget:** £615,000
- **Funding:** EPSRC
- **Centre lead:** Professor Steve Schneider
- **Partners:** Kings College London, Civica Election Services, Crowdcube, Monax Industries
- **Timeframe:** 2017-2021



Completing Your Vote

To complete voting click on the SEND MY VOTES button below. ALERT! Once you send your votes you CANNOT change how you voted.

DECaDE

(Centre for the decentralised digital economy)

In our increasingly decentralised digital economy, everyone has the opportunity to be both a producer and consumer of goods and services but, because these peer-to-peer markets are underpinned by centralised digital platforms, users rarely have a say in their governance decisions.

DECaDE is a national hub which aims to use distributed ledger technology and artificial intelligence technologies to transform this emerging economy into one that has fair governance and maximises opportunities for everyone to create value. Initial areas of research include fake news around Covid-19 vaccination and supply chain visibility. In January 2021 DECaDE also held its first workshop with industry partners, focusing on the creative sector, to kickstart co-created research projects.

- **Budget:** £4m, plus over £6m contribution from industry
- **Funding:** UKRI/EPSRC
- **Centre lead:** Professor Steve Schneider
- **Partners:** Centre for Vision, Speech and Signal processing, Centre of Digital Economy, University of Edinburgh, Digital Catapult
- **Timeframe:** 2020-2025

Find out more about DECaDE: decade.ac.uk/

Scalable and resilient data replication for distributed ledgers and blockchains

Every party participating in a blockchain network has its own copy (or 'replica') of the chain, which enables them to independently verify the legitimacy of the transactions, enforcing the key blockchain promise of 'decentralised trust'. This creates a challenge when it comes to large-scale distributed block replication at a large scale involving complex distributed protocols, as these must be both secure and able to scale to potentially tens of thousands of participants.

In this project, SCCS is collaborating with IBM to design these protocols in the specific context of HyperLedger Fabric – the key blockchain technology being developed by IBM. The project has generated a number of high profile breakthroughs, with research published at ACM Systor 2017, the International Symposium on Distributed Computing (DISC) in 2018 (winning the best paper award) and 2020, and Springer Distributed Computing journal 2021.

- **Budget:** £22,300
- **Centre lead:** Professor Gregory Chockler
- **Partner:** IBM
- **Timeframe:** 2017-2024

COMMUNICATION AND NETWORKS

WITH THE EMERGENCE OF THE INTERNET OF THINGS AND ULTRA-HIGH SPEED MOBILE AND WIRELESS CONNECTIVITY ON THE HORIZON, FUTURE COMMUNICATIONS AND NETWORKS NEED TO INCORPORATE NOVEL PROTECTION MECHANISMS TO ENSURE SECURITY, RELIABILITY, AND ADEQUATE FAULT TOLERANCE. SCCS COLLABORATES CLOSELY WITH SURREY'S 5G INNOVATION CENTRE TO BUILD SECURE COMMUNICATION SYSTEMS IN SECTORS SUCH AS CONNECTED VEHICLES AND DIGITAL HEALTHCARE.

ESKMARALD

ESKMARALD looks at the cryptographic, security and privacy guarantees of edge computing over mobile networks and related services, primarily as per 5G (5th Generation Mobile Network)-related specifications. ESKMARALD considers different threat models, as well as by using various formal analysis methods and tools for security protocols and cryptographic primitives. Where appropriate, patches will be proposed and formally studied in turn.

Within the realm of edge-computing security, we are particularly interested in the AKMA (Authentication and Key Management for Application) service in 5G, which we will comprehensively analyse within the ESKMARALD frameworks.

Alongside the main security-centred endeavours of the project, we are working with BT on practical aspects of AKMA deployments and variations on its implementations in 5G simulation/test-bed environment.

- **Funding:** NSCS (National Cyber Security Centre)
- **Centre lead:** Prof. Ioana Boureanu
- **Co-Investigators:** Prof. Schneider, Prof. Helen Treharne, Dr. Mohammad Shojafar (from Surrey's 6GIC/ICS).
- **Timeframe:** November 2022 - November 2024

SOCIAL MEDIA /PRIVACY

PROBLEMS ASSOCIATED WITH SOCIAL MEDIA USE HIT THE HEADLINES EVERY DAY – FROM TEENAGE BULLYING TO TROLLING AND HATE SPEECH – BUT PUTTING IN PLACE MEASURES WHICH EFFECTIVELY REMOVE FREE SPEECH NEEDS CAREFUL CONSIDERATION. WE APPLY DATA ANALYSIS TO UNDERSTAND ONLINE HARM IN SOCIAL NETWORKS IN ORDER TO DEVELOP BETTER SYSTEMS AND ARCHITECTURES, AND DRIVE SOCIAL AND PUBLIC POLICY IMPACT.

Characterising hate speech in MPs' and citizens' conversations

With 650 MPs now on Twitter, interpreting how citizens engage with them online has become fundamental to understanding modern democracy in the UK. In collaboration with the House of Commons Library Research team, SCCS is examining how MPs and citizens engage online in order to understand whether the negative emotions being expressed in these conversations have elements of hate speech and, if so, whether this is across party political divides, or due to ideological differences within a party. As part of the project, hate speech meta tools developed by SCCS and the Alan Turing Institute will be applied to this nationally important dataset.

- **Centre lead:** Professor Nishanth Sastry

AP4L (Adaptive PETs to Protect and emPower People during Life Transitions)

AP4L aims to study and mitigate online privacy & vulnerability challenges that people face when going through major life transitions. Our central goal is to develop privacy-by-design technologies to protect & empower people during these transitions.

AP4L aims to introduce a step-change, making online safety and privacy as painless and seamless as possible during life transitions. We will achieve this through the development of a suite of technologies and solutions that will help people navigate significant life transitions through adaptive, personalised privacy-enhanced interventions that meet the needs of each individual and bolster their resilience, autonomy, competence and connection. The suite will comprise:

- "Risk Playgrounds", which will build resilience by helping users to explore potentially risky interactions of life transitions with privacy settings across their digital footprint in safe ways
- "Transition Guardians", which will provide real-time AI-based protection for users during life transitions.
- "Security Bubbles", which will promote connection by bringing people together who can help each other (or who need to work together) during one person's life transition, whilst providing additional guarantees to safeguard everyone involved.

- **Budget:** £3.44 million
- **Funding:** Engineering and Physical Sciences Research Council
- **Centre lead:** Professor Nishanth Sastry
- **Co-Investigator:** Prof. Steve Schneider, Prof. Helen Treharne, Dr Constantin Cătălin Drăgan, Dr Suparna De

APPLIED CRYPTOGRAPHY

WITH OUTSTANDING EXPERTISE IN THIS FIELD, WE FOCUS ON ADVANCED CRYPTOGRAPHIC TECHNIQUES AS AN INTEGRAL PART OF MANY OF OUR PROJECTS – AS CAN BE SEEN THROUGHOUT THE PROJECT PAGES OF THIS BROCHURE. THE TECHNIQUES WE USE INCLUDE HIGH FUNCTION ENCRYPTION SCHEMES AND DIGITAL SIGNATURES, AUTHENTICATION AND KEY EXCHANGE PROTOCOLS, AND CRYPTOGRAPHIC SOLUTIONS FOR PRIVACY-PRESERVING IDENTITY MANAGEMENT, SECURE DATA SHARING AND INFORMATION EXCHANGE.

GLOBAL AUTHORITIES ON CRYPTOGRAPHY

Core members of SCCS, Professor Liqun Chen, Dr Robert Granger and Dr Jack Tian are three of the academics leading the Centre's research into hardware security and cryptography.

Professor Liqun Chen has invented or coinvented cryptographic solutions which have been incorporated into international standards and used in applications millions of people use every day. As principal research scientist in the Security and Manageability Laboratory at Hewlett Packard Labs, she was instrumental in developing the Trusted Platform Module (TPM), a hardware chip that ensures security by integrating cryptographic keys and algorithms in devices. She has since led development of a Quantum-Resistant TPM (see page 9).

Dr Robert Granger is a world-renowned computational number theorist who has made important breakthroughs in foundational cryptographic security assumptions. He has designed highly original discrete logarithm algorithms for various algebraic groups and has set several world records for discrete logarithm computations. In 2019, he was part of a team of researchers to hail the end of a variant of a cryptosystem that is widely used to protect online transactions, by solving a 30750-bit discrete logarithm problem using a quasi-polynomial time algorithm; this beat the previous record of 9234 bits set in 2014.

Dr Jack Tian is a cyber security expert who has made enormous contributions to applied cryptography. He has designed several chameleon-hash schemes to secure blockchain rewriting systems, including a new chameleon-hash function that supports accountable blockchain rewritings. He also designed many privacy-preserving user authentication schemes and key exchange protocols that can be used to support IoT systems securely and efficiently.

PKC-SEC

(Security Analysis of Classical and Post-Quantum Public Key Cryptography Assumptions)

PKC-SEC aims to research and develop algorithms for solving computational problems that are foundational to the security of PKC, both now and in the future. As a result of Shor's breakthrough algorithms for solving the IFP and DLP on a sufficiently large quantum computer, replacement post-quantum (PQ) cryptosystems have been studied in earnest for the past 15 years, with standardisation efforts in process by both NIST and ETSI. PQ cryptosystems must be secure against both classical and quantum computers and therefore their underlying hardness assumptions must be studied intensely before they can be fully trusted to replace our existing PKC hardness assumptions. Until these standards have been established and cryptographic practice migrates entirely to PQ cryptography, it is also essential that the study of classical hardness assumptions persists, particularly as sporadic and sometimes spectacular progress can occur, as demonstrated by previous results of Dr. Granger. PKC-SEC will deepen our understanding and assess the hardness of three natural and fundamental problems, thus providing security assurances to the cryptography community and more generally all users of cryptography.

- **Budget:** £298,000
- **Funding:** UKRI/EPSRC
- **Centre lead:** Dr. Robert Granger
- **Partners:** Ethereum Foundation, Katholieke University Leuven (COSIC), PQShield
- **Timeframe:** January 2023 to December 2024

STUDY AT SURREY

THE UNIVERSITY OF SURREY IS AN ACADEMIC CENTRE OF EXCELLENCE IN CYBER SECURITY EDUCATION (ACE-CSE) AND OFFERS A RANGE OF STUDY OPPORTUNITIES WHICH ARE INFORMED BY OUR GROUND BREAKING RESEARCH ACTIVITIES.

MSc in Information Security

Our GCHQ-certified **MSc in Information Security** (surrey.ac.uk/postgraduate/information-security-msc) is designed to equip students with the theoretical knowledge and hands-on experience necessary to pursue a successful career in cyber security. The course covers the foundations of systems and information security such as cryptography, and also advanced concepts such as the inner workings of electronic payments and distributed ledgers.

Students also have the option of undertaking a placement year, drawing on the University's strong, established links with leading national and international organisations.

In addition to our MSc in Information Security, which is specifically designed to train students for a career in cyber security, specialist cyber security modules are embedded in our undergraduate degrees and other masters courses. There are also opportunities to undertake a PhD – often sponsored by industry or government – to explore specific aspects of cyber security.

Find out more about our computer science courses: surrey.ac.uk/subjects/computer-science

WHAT OUR PHD STUDENTS SAY

My PhD project, funded by NCSC, investigates more flexible approaches to authentication (account security) on the web using new standards from W3C and the FIDO Alliance, who develop technologies for using standalone authentication devices, such as YubiKeys, as well as built-in authenticators (e.g., fingerprint scanners, Apple's Face ID). An ongoing issue is that the loss of an authenticator or device may result in losing access to online accounts. Our first paper (ACM CCS 2020) investigated how to share keys securely amongst authenticators, allowing for backup authenticators to be used with online accounts, and our more recent result (ESORICS 2022) extended this to sharing credentials with other people securely

Nick Frymann

My PhD, supervised by Prof. Brijesh Dongol, is funded by VETSS (Verified Trustworthy Software Systems) and focuses on verifying concurrent programs under non-volatile/weak memory models. In particular, I am using theorem proving (Isabelle/HOL) to reason about weak memory models, persistency semantics, and persistent software transactional memory algorithms. Our paper "View-Based Owicki–Gries Reasoning for Persistent x86-TSO." has recently won a Distinguished Artifact Award at ESOP 2022.

Eleni Valfiadi Bila

SURREY CENTRE FOR CYBER SECURITY
University of Surrey
Guildford, Surrey GU2 7XH, UK

+44 (0)1483 68 6058
SCCS@surrey.ac.uk
surrey.ac.uk/sccs
Twitter: @SCCS_UniSurrey

LEARN MORE

Discover more about our research projects:
surrey.ac.uk/surrey-centre-cyber-security/research

Find out about our MSc Information Security:
surrey.ac.uk/postgraduate/information-security-msc

UNIVERSITY OF SURREY