Institution: Royal Holloway, University of London

Unit of Assessment: 11

1. Unit context and structure, research and impact strategy

1a. Overview

Our unit combines the research strengths of Computer Science (CS) and Information Security Group (ISG). Both Departments have significantly expanded over the assessment period with 41 academics submitted to REF2021 (26 in REF2014). The unit is within the School of *Engineering, Physical and Mathematical Sciences* (EPMS), part of the College-wide six-School structure created in 2019. Staff are co-located in the newly refurbished Bedford Building, a prioritised £5.9m investment. This physical environment promotes collaboration, efficiency and hosts state-of-the-art computing resources and advanced laboratories, supported by cutting-edge cloud infrastructure.

The unit's diverse portfolio of inter-related activity ranges from well-established excellence in Algorithms, Machine Learning (ML) for Big Data, and Cybersecurity, including Post-quantum Cryptography, to strongly developing research in Artificial Intelligence (AI) and Robotics. The vibrancy of our environment is enhanced by a demographic in which 38% of submitted academics are ECRs (28% women), with 40% of academic staff joining since 2014. The unit's commitment to an equitable and sustainable future in the field is also represented by the pioneering role it plays in PGR training, including the current CDT in Information Security, which is the third in a consecutive series begun in 2013, with cumulative funding of £13.2m. Through its Equality, Diversity and Inclusion policies it can boast a diverse annual cohort (currently 60% women, 40% on average) which will contribute to improved gender balance in the next generation of experts. An overview of strategic improvements since the last REF is depicted in Fig. 1.

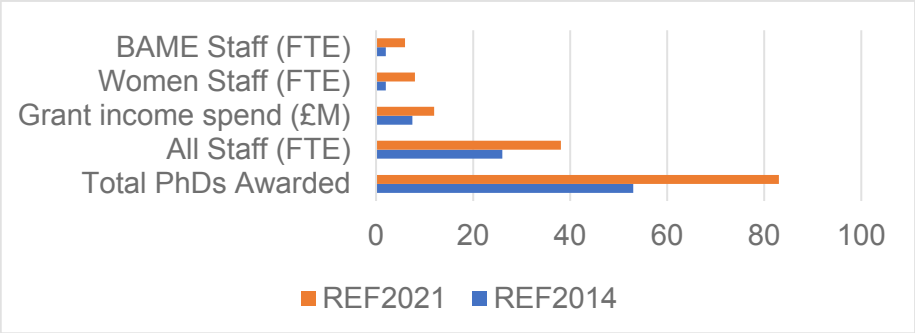

Figure 1: *REF2014 vs REF2021*

As part of the Royal Holloway (RHUL) Strategy 2020-2024, the unit is playing a key role in two of the four catalyst research and knowledge exchange hubs. The Transformative Digital Technologies, Security and Society catalyst rests on the technological pillars developed from intertwining AI/robotics and information/cyber security, together with the other research strands discussed in detail below. The Advanced Quantum Science and Technologies catalyst will harness leadership in post-quantum cryptographic algorithms to protect legacy systems, while developing research on algorithms and quantum resource estimation for quantum computers. Both catalysts align with UKRI strategic priorities and will address fundamental research as well as real-world industrial and societal challenges.

This unit is positioned to take full advantage of new opportunities and is well supported by RHUL's investment and strategy.

1b. Unit Structure

In REF14 we promised to retain our organisation and extend it with synergies in cloud computing for big data, systems security, distributed systems and ML, and new interdisciplinary activities in socio-technical security. To implement our REF14 strategy we extended our four CS centres and expanded our ISG activities with three thematic sub-groups, as shown in Fig. 2. The Centre for Algorithms and their Applications (CAA) focuses on the theory and applications of parameterised algorithms and solving problems previously too complex to tackle computationally. The Computer Learning Research Centre (CLRC) encompasses foundational studies in learning from data, with emphasis on reliable predictions for practical applications. Research within the Centre for Software Language Engineering (CSLE) ranges from traditional programming language design and implementation to customised computer architectures for embedded systems. The Centre for Distributed and Global Computing (CDGC) addresses theoretical and practical challenges in large-scale and dynamic distributed systems, with autonomous agents and intelligent capabilities such as automated planning. The Cryptography group, overlapping with Mathematics, focuses on designing, evaluating and implementing cryptographic algorithms and protocols. The Systems and Software Security Lab (S3Lab) studies how software vulnerabilities are introduced and exploited, and designs novel mitigation techniques to address them. The Social and Cultural aspects of Information Security explores technical issues overlapping with social sciences.

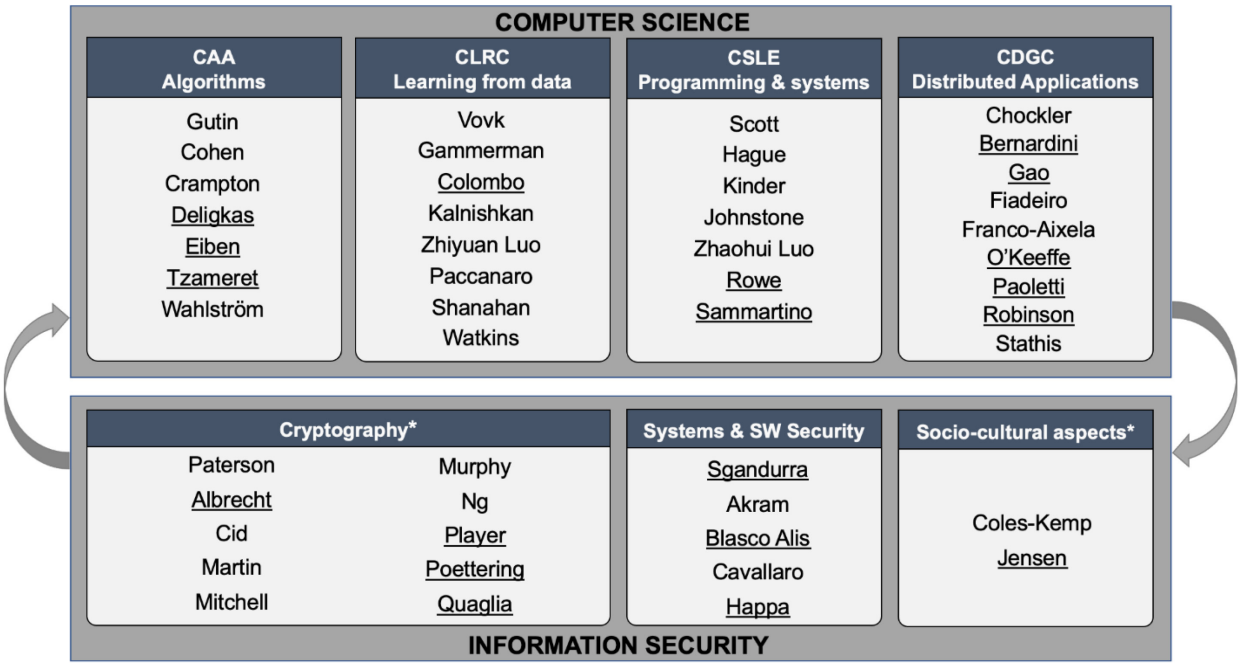

Figure 2: *Staff categories A&B with new appointments (underlined) and interdisciplinary work (*)*

1c. Research objectives

Our research and impact activities, and the development of our staff and research environment have been directed by *three strategic objectives*, to deliver our REF14 strategy. These objectives, and a selection of highlights to illustrate achievements are:

- ***To study fundamental problems of computation and information security, develop novel theoretical models and frameworks, investigate their properties and impact their related research communities.***

  The cross-cutting challenges that we targeted are (i) new parameterized algorithms and input compression algorithms for theoretical and practical problems, including those in information security (ii) novel theoretical models that translate data to knowledge ranging over a number of

topics, from large scale data-management, prediction models with validity guarantees, autonomous systems models with planning and reasoning capabilities (iii) novel cryptographic models for lattice-based and post-quantum cryptography which linked us to the UK Quantum Technology Hub for Quantum Communications Technologies.

- ***To develop innovative computational and information security mechanisms and open solutions for practical single and multidisciplinary applications to benefit society, business and national security.***

Some of the diverse areas at spotlight include: (i) semi-supervised learning for disease prediction and a novel algorithm for predicting biological processes ranked 1st in the CAFA-16 competition on protein function prediction (ii) medical applications for diabetics patients and a controller that regulates the operation of an artificial pancreas (iii) work on autonomous UAVs for search and rescue and strategies intelligent agents can adopt for negotiating in e-markets (iv) a security engagement toolkit that has been adopted by the National Cyber Security Centre and used by security practitioners, civil society and teachers.

- ***To offer advice and provide knowledge transfer to impact government and industry through technical innovation and commercialisation.***

Examples of our strategic priorities include: (i) working with British Gas to improve their Big Data analytics, and helping AstraZeneca to devise ML methods for drug discovery (ii) providing cybersecurity consultancy services to a wide range of clients, such as governments, transport operators, telecoms, standards bodies, private companies, and innovative start-ups (iii) an ISG member is the Deputy Director of the UK's Research Institute for the Science of Cyber Security (iv) being instrumental in the creation of the *All Party Parliamentary Group on Cyber Security* and providing the secretariat ever since, arranging Westminster discussions to benefit parliamentarians and positively influence national policy.

We have operationalised the above objectives with mechanisms that stimulate new grant income for a variety of collaborative projects (investigators Albrecht, Bernardini, Sgandurra, Gutin, Gammerman, Vovk), often inter-disciplinary (investigators Coles-Kemp, Paccanaro), and supported by diverse funding sources (section **3a**). Since 2014, we have also responded to new challenges in computing and information security research (section **1d**) reinforced by investment in people to sustain our research groupings (section **2a**) and infrastructure (sections **3b** and **3c**). Strategy is discussed in research committees with all staff invited, and changes take place annually, in awaydays for both CS and ISG, where adjustments/revisions are agreed. Since 2019, strategic changes are coordinated by the Research and Knowledge Exchange Committee, chaired by the EPMS Research Director and attended by Research Leads and ECR representatives of School Departments.

1d. Research strategy 2014-20

The **Centre for Algorithms and Applications (CAA)** contributes to our first research objective. Funded by EPSRC (EP/K005162/1, £602,797) and Leverhulme (RPG-2018-161, £209,740), Cohen, Crampton and Gutin have focused on the Workflow Satisfiability Problem resulting in best paper awards in 20th and 21st ACM SACMAT. Work on Parameterized Algorithms, funded by Gutin's *Royal Society Wolfson Research Merit Award* (£75,000) and Wahlström's EPSRC (EP/P007228/1 £100,847), solved four open problems in combinatorial optimization and parameterized complexity and a more than thirty years open question with practical significance. Wahlström received the *EATCS-IPEC Nerode Prize 2018* for settling the long-standing open problem about the polynomial kernelizability of the Odd Cycle Transversal problem. Cohen and co-authors published several results on the complexity of (valued) constraints and won the journal

track paper award at CP. Tzameret's research on Theoretical Complexity studied fundamental lower bounds in proof complexity (funded by NSFC/61373002, ~£100,000) and novel algebraic approaches. With colleagues, Tzameret resolved a long-standing open problem, establishing short propositional proofs for the determinant identities, which paved the way to establish with S. Cook (inventor of NP-completeness) a minimal theory in which linear algebra can be developed.

The **Centre for Distributed and Global Computing (CDGC)** contributes to our first two objectives. Funded by IBM, work in resilient and trustworthy computing by Chockler and colleagues received best paper in DISC18. O'Keefe, with IBM and Imperial, proposed novel algorithms to support data-parallel stream processing and efficient recovery from transient network failures. In Autonomous Systems for Uncertain Environments, Bernardini obtained ~£0.9M from Innovate UK. With Toronto and EPSRC funding (EP/S016473/1) she developed new UAV techniques locating a moving target, while her work in planning won best paper honourable mention award in ICAPS20. With EU funding (FP7-ICT 287841, £342,831) Stathis developed agents monitoring diabetic patients using smartphones. He also established negotiation heuristics for e-markets and, with Paoletti, used them to learn adaptive strategies using Deep Reinforcement Learning. Paoletti and colleagues in Oxford developed the first method for synthesis of stochastic chemical reaction networks, relevant beyond the biological domain.

The **Computer Learning Research Centre (CLRC)** contributes to all our research objectives. In ML theory Vovk extended conformal prediction from set predictions to predictive distributions and Gammerman extended Venn prediction to predictive distributions. Both extensions facilitate applications of previous CLRC-developed work to decision-making. Kalnishkan developed aggregating algorithms to scenarios with multiple outcomes occurring at the same time (Leverhulme, £113K). Watkins developed genetic algorithms that satisfy detailed balance (FP7-ICT-270327, £266,427). Zhiyuan Luo and Watkins developed a novel tracking location mechanism for public transport on mobile devices, without using GPS. Paccanaro's lab ranked 1st in the CAFA-16, an international competition on protein function prediction involving 126 methods from 56 research groups. They also analysed network evolution of protein complexes through time in plants (NSF/BIO-BBSRC, £583,852). Zhiyuan Luo was one of the first to annotate an armed conflict database of Iraq and to apply ML to conflict analysis. Gammerman developed predictive maintenance models for British Gas (Centrica, £60,000), and with Zhiyuan Luo and Vovk developed conformal prediction for drug development (EU, £278,383, and AstraZeneca, £395,762).

The **Centre for Software Language Engineering (CSLE)** contributes to all our research objectives. Funded by EPSRC (EP/I032509/1, £491,077), Scott and Johnstone developed the first fully general parsing technique that can directly implement the more concise and user preferred extended BNF language for grammar specification in collaboration with teams in Eindhoven, Delft and CWI Amsterdam. Using his EPSRC Early Career Fellowship (EP/K009907/1, £469,677) on Verification of Automata, Hague developed with Beijing, Uppsala, and others the theoretical foundations and state-of-the art implementations for constraint solving algorithms, supporting the first robust key operations on strings. He has also applied, with Oxford, verification techniques to web-site optimisation, formalising cascading style sheet (CSS) semantics and providing minimisation techniques for standalone CSS. In the area of Natural Language Semantics and Subtyping, Zhaohui Luo and colleagues have invented and developed Modern Type Theories (MTT) semantics, which have made a significant contribution to the field of formal semantics (Leverhulme F/07-537/AJ 148K, Royal Academy of Engineering 1314RECI027 10K, and EU Cost action CA15123 with 29 countries).

The Information Security Group (**ISG)** contributes to all research objectives. In the **ISG cryptography** (thematic-group), Albrecht's work on lattice-based coding and cryptography (EP/S020330/1, 2019, £482,051; EP/S02087X/1, £379,964 and EU H2020 780701, with Paterson; total project £397,433) has yielded important results on core constructs such as learning with errors (with R. Player) that have been cited extensively. Paterson's fellowship on 'Cryptography: Bridging theory and practice' (EP/H005455/1, £1,239,093) focused on block cipher modes of operation, timing, and pseudo-randomness, and resulted in top-tier publications, best paper at ACM CCS'16 and influencing the widely used IETF TLS protocol. Work on cryptanalysis (Poettering) received best paper at Crypto'19. Post-quantum and lattice-based cryptography research combined (with additional grants EP/P009417/1, EP/L018543/1) totals ~£1.46M and identifies, inter alia, the ability to rely on a subfield to solve overstretched versions of the NTRU assumption in lattice problems; this research linked the ISG to the UK Quantum Technology Hub for Quantum Communications Technologies (EP/M013472/1).

The **Systems and Software Security Lab (S3Lab)** originated from Cavallaro collaborating with CS (Gammerman, Zhiyuan Luo, Shanahan and Vovk) to detect malware behaviour, malware behaviour reconstruction and mining (EP/K033344/1, EP/L022710/1, EP/L022710/2, ~£1.67m shared between the two Departments). This activity has been strengthened through new hires across S3Lab and ML. Sgandurra is part of an international consortium for developing a next generation Trusted Platform Module, which is embedded to make the host computer of a system trustworthy and secure (H2020 FutureTPM, GA-779391, RHUL £320,000, total ~£4.2M). Blasco-Alis and colleagues developed a declarative strategy for detecting collusions on Android and demonstrated how to discover collusions over 50,000 apps. Similarly, Happa and colleagues from Oxford, showed how sonification can solve some network monitoring challenges in security operations centres and reported significant performance improvements when sonification was used.

The development of research on **Social and cultural aspects of Information Security** has been an important strategic direction, identified in REF14. Our work is well-aligned with and has helped to drive national priorities. Coles-Kemp's work funded by EPSRC (EP/K006266/1, ~£750,000) and EU FP7 (Grant No. 318003, ~£350,000) has developed a security visualisation tool kit that can be used by security practitioners to both widen engagement in risk assessment, audit and security training and to identify how the social and cultural aspects of an organisation affect security practices. The National Cyber Security Centre has adopted and promoted this toolkit through its people-centred security guidance: You-Shape Security. Coles-Kemp's fellowship (EP/N02561X/1, ~£775,000) supports her interdisciplinary work with Jensen for developing a critical approach to analyse digital security practices. Their approach makes policy recommendations based upon a better understanding of security technology barriers in marginalised communities and has received recognition by the CHI community.

1e. Supporting interdisciplinary research

Interdisciplinary work is reflected in our research objectives, structures and research permeating CS, ISG and Mathematics. Our activity spreads beyond these Departments through College interdisciplinary Doctoral Centres (e.g., the Leverhulme DTC and AHRC Techne) and interdisciplinary clusters (e.g. the AHRC StoryFutures). Our recent CDT led by ISG involves collaboration with Departments of Geography, Psychology, Economics, Politics, EE, CS and Mathematics. ISG also links anthropological studies of security engagement according to gender and social status (Coles-Kemp and Jensen). CS has always maintained close links with Biologists internationally (e.g., Paccanaro and colleagues in Yale). Work in Finance by Vovk has been carried

out with Economics, while activities by Johnstone and Scott have contributed to the Heritage sector. Stathis with Gao and our School of Law have applied AI to improve the 'fitness to practise' process for UK, Australian and US regulators.

1f. Approaches to enabling Impact

Our ISG was founded to engage with industry and government (1990) and was recognised by a Queens's industry award (1998). We have built upon this legacy as a unit, with a diversity of funded activities, as well as engaging external experts in research-led teaching, relevant to the world challenges of today. Our approach incorporates the following strategic directions.

Responding to Industry Needs: A 30+ year association with Hewlett Packard, celebrated by the annual HP-Day event, has focussed on real-world application of cryptography. An association with Vodafone and Giesecke & Devrient led to the creation of the Smart Card Centre, now re-positioned as the Smart Card and IoT Security Centre. The S3Lab creation was supported by McAfee/Intel. A formalised engagement via an Industry Advisory Board in CS, established in 2011, tackles shared strategic issues through open dialogue with our industrial partners. Board members represent organisations such as Accenture, Blackrock, BT, Deutsche Bank, Salesforce, IBM, Gartner, Shell, Fujitsu and Spotify. The board advises on the industrial relevance and suitability of our teaching and research. We continue to influence standardisation bodies such as the IETF, BS, ISO and ETSI. Our best response to industry is exemplified by our TLS security impact case (Paterson), addressing the needs of companies such as Google and Apple.

Responding to Government Needs: We influence and stay abreast of evolving needs in government and society, thus allowing us to adapt to satisfy them. We have been fully engaged with GCHQ/NCSC strategy to expand academic activity in cybersecurity. We were one of the first units to become a recognised Academic Centre of Excellence in Cyber Security Research (ACE-CSR) and to gain NCSC approval for our MSc in Information Security, and we were the first to offer an NCSC approved BSc, in Computer Science with Information Security. We are also very active in government policy making, via NCSC and DCMS, policy think-tanks, parliamentary groups, strategy groups, and via our societal research activities. Evidence of our successful response to government needs is our case study with creative securities (Coles-Kemp).

Rewarding Intellectual Property creation: We encourage all staff to identify, protect and consider exploitation, of their research innovation (R&I). Our R&I office in collaboration with research directors and experienced staff with patenting and commercial experience, act as advisors on promising work. Rewarding staff for successful commercialisation is a foundation principle of our intellectual property (IP) policy. IP creation and exploitation are promotion factors. Exploitation is not always directly commercial; in information security, the contribution of innovation to peer-reviewed and openly available algorithm and protocol standards (e.g. for the Internet) has massive security and financial impact. Innovation through IP creation and exploitation is also impressed on our research students and assistants (e.g., our CDT offers guest lectures on IP and innovation for PhD students).

Industrial Collaborations: Most of our research includes collaborations with industry, e.g., through partnership in UKRI and EU projects, but we also use direct industrial funding. We give some examples here. Cid's and Albrecht's work on post-quantum cryptography has been used by TLR Technology Ltd to develop a novel hardware implementation of post-quantum cryptographic schemes. Kalnishkan and Watkins apply ML techniques for trading with the start-up AlgoLabs (founder a CS alumnus) supporting systems for Divisa Capital Ltd and Equiti Global Markets. Johnstone's and Scott's GLL parsing algorithms research has been adopted by SonarQube, a very successful continuous code quality tool adopted by major development projects from organisations

such as eBay and BMW. The most fruitful industrial collaborations are reported in our impact cases with IBM (Chockler) and AstraZeneca (Gammerman et al).

Consultancy: Staff are encouraged to capitalise on their expertise by undertaking external consultancy, working through our R&I office. The ISG staff have carried out confidential, security sensitive work in various sectors including communications, transportation, government, finance and payment, legal, and devices. Recent consultancy work related to post-quantum cryptography is designed to set future standards, with a massive impact potential worldwide. Since 2014, we have participated in 34 consulting projects with 26 external clients; these include private individuals, high-tech start-ups and large multinationals such as Softmorphis, Greycon, KPMG, Thales, British Gas and BAE.

PhD Students: Our students are employed in organisations such as Amazon, Blackrock, Cloudflare, Facebook, Google, HP Inc, JP Morgan, Microsoft Research, Mozilla Foundation, Nomura, and Yahoo. This is a powerful mechanism for transferring our research, especially into the UK industrial base. CDT students are exposed to a variety of companies via lectures and organised visits and go on to participate in internships as part of their studies. We also provide female role models, for impact research, with the visiting professor appointments of Whitty and Ashenden. These measures are bearing fruit as a team of women students won the InfoSec prize for best cybersecurity students.

1g. Research and Impact strategy 2021-2026

Our research and impact strategy is supported by a diverse portfolio of active academic and industrial collaborations (section **4**). The established centres have strong trajectories building on their research strengths and aligned with our strategic goals. The large influx of academic staff in the REF2021 period is an important driving force. Supporting their strongly developing research (section **2**) will contribute to shaping this future.

To further promote multidisciplinary research and impact, aligned with UKRI priorities, our organisation framework is currently being modified with several new initiatives.

The potential for multidisciplinary collaboration on AI across the new College-wide Catalyst Transformative Digital Technologies and Society will be enhanced by initiating a Centre for Intelligent Systems. This will build on our expertise in applied ML and model-based AI to complement the work of Computer Learning Research Centre, which will focus on reliable ML. The technological pillars for the catalyst will be our strengths in AI/robotics and information/cyber security, linked to other research strands. This will be coupled to the human and social aspects of ISG and CS, which will also be strengthened. Combining all these areas in the Catalyst with distinctive research strengths in psychological, societal, economic and environmental contexts across College, we will promote widest possible impact of our capability and expertise. Research on post-quantum cryptography will be integral to the Advanced Quantum Science and Technology Catalyst.

We will also build upon the capabilities of the S3LAB and create more project-level linkages with ISG's Security and Smart Card centre (returned with RHUL's Engineering submission), giving our future research a solid basis in software and hardware security.

1h. Sustaining an open research environment and reproducibility of research

We operationalise knowledge transfer (third research objective), by contributing to open standards, open-source libraries, and open-source projects. Albert is maintainer and author of the LWE Estimator for assessing lattice-based cryptography (the de facto tool for the Homomorphic Encryption Standard used by industry, government and academia). He is also maintainer and

developer for lattice reduction libraries FPLLL (143 GitHub stars) and FPYLLL (43 GitHub stars) used to analyse post-quantum schemes, fully homomorphic encryption schemes and to perform side-channel attacks. Moreover, he is a credited developer of SageMath, a free viable alternative to Mathematica, Maple, Magma and Matlab (1.2k GitHub stars). Hague collaborates on SatCSS, a tool for minifying CSS stylesheets using constraint solving to discover semantics-preserving rule merge operations (11 GitHub stars). Franco-Aixela has contributed four planners (Complementary 1&2, Planning-PDBS, Meta-Search Planner, and RIDA) to the International Planning Competition (IPC) website. Complementary 1&2 was runner up at IPC-18.

We aim beyond typical open access, as cryptographic algorithms and protocols undergo peer-review, to avoid security-by-obscurity. Security standardisation also has strong preference for royalty free usage. Mitchell's great service in this area includes ISO/IEC/BS/NIST/ITU and ETSI. We are also expanding our ambitions for open-data sharing, through our membership of the International Cyber Security Centre of Excellence (INCS-CoE). Workgroup 2 of INCS-CoE is devoted to international policy, affecting the cross-border free flow of data, information sharing and privacy; institutions are involved from Australia, Israel, Japan, UK and USA. We target open-data sharing, depending on legal collaboration agreements e.g., Zhiyuan Luo and colleagues describe the first Iraq Body Count Corpus dataset, as the first armed conflict-related dataset open for analysis. Furthermore, we influence international reproducibility e.g., Shanahan (Professor of Open Science) contributes to the `CODATA-RDA Schools for Research in Data Science' initiative.

2. People

2a. Staffing strategy

To deliver our strategy, we have developed and expanded the established research groups, summarised in Fig. 2, strengthening synergies between the growing areas of Algorithms, AI/ML, Programming Languages and Information Security. Expanding the unit has been an institutional priority. Over the assessment period our significant growth has emphasized the recruitment of ECRs with potential to become future research leaders. All new appointments, by gender balanced panels trained in unconscious bias, have been at lecturer level, and have improved gender equality.

In CS we have expanded our Centre for Distributed and Global Computing with AI planning for autonomous systems (Bernardini/King's), cyber-physical systems (Paoletti/Stony Brook), large-scale distributed systems with links to systems security (O'Keeffe/Imperial) and natural language processing (Gao/TU Darmstadt). We have also strengthened our Centre for Algorithms in computational complexity (Tzameret/Tsinghua), parameterised algorithms (Eiben/Vienna), and algorithmic game theory (Deligkas/Liverpool). We have reinforced the Centre for Software and Language Engineering in formal verification (Rowe/Kent and Sammartino/UCL), and supported ML Research in multi-dimensional data analysis (Colombo/UCL).

In ISG, we have strengthened the Cryptography group with cryptanalysis and post-quantum cryptography (Albrecht/DTU and Player/RHUL), as well as identity-based and attribute-based encryption (Quaglia, Huawei Technologies), shifting the emphasis of research following the departure of Paterson to ETH (Zurich) in 2019. The successful establishment of capability in Software and Systems Security (S3LAB), driven originally by Cavallaro (who left to KCL), has been consolidated and built on by three hires by strengthening; malware systems research (Sgandurra/Imperial and Happa/Oxford); mobile applications security (Blasco-Alis/City), supported by hiring O'Keeffe. Multi-disciplinary research driven by Coles-Kemp in the social and cultural security area in collective security practices has been expanded by (Jensen/RHUL).

As a measure of the success of this strategy for sustainability, 46% of our existing staff were promoted, including many who were recruited as ECRs. To Senior lecturer - Blasco-Alis, Jensen, Ng and Quaglia; to Reader – Cavallaro, Sgandurra; to Professor - Albrecht, Bernardini, Cid, Coles-Kemp, Hague, Zhiyuan Luo, Paccanaro, Shanahan, Stathis, Tzameret, Wahlström and Watkins. High levels of retention also contribute positively to this healthy demographic. Only three of our senior academics left to other British institutions: Cavallaro to King's; Chockler to Surrey; Fiadeiro to become Dean of Science and Engineering at Dundee. Long service is common, and Crampton left by retirement.

Paterson held an EPSRC Leadership Fellowship (until May 2015), Coles-Kemp an EPSRC Digital Economy Fellowship (2016-2021), Hague an EPSRC Early Career Fellowship (2013-18). Tzameret was awarded an ERC Fellowship in December 2020.

Our staffing and recruitment policies focus on merit, and on at least two occasions this has meant recognising untapped research talent in our teaching-only contract staff. Blasco-Alis made this transition and is now a driving force within the S3LAB, as did Jensen who is now carving a strong reputation in the human-factor/societal research. We also strive for better gender equality. In ISG for example, we have increased the number of permanent, research-active, women staff by 150% (2 to 5) since the last REF, adding Jensen, Quaglia and Player. We also appointed two women, Whitty and Ashenden, as ISG Honorary Professors. This is in part due to having Coles-Kemp as role model, within ISG's human-factors domain.

This strategy has paved the way for: establishing a new Centre in Intelligent Systems; playing a pivotal role in establishment of the Transformative Digital Technologies, Security and Society catalyst; and contributing to the Advanced Quantum Science and Technologies catalyst.

2b. Staff development strategy

New staff join an appropriate centre and have a trained academic mentor, who represents them at three annual probationary reviews. They have a reduced teaching load (50%) in the first year. RHUL is committed to the career development of staff at all levels. In 2019 we received the HR Excellence in Research award, demonstrating our commitment to the principles of the UK *Concordat to Support the Career Development of Researchers*. A key of the developmental programme is 'Advance', providing training for researchers contributing to deliver of this commitment. 'Advance' also includes mandatory sessions on research integrity and research ethics. Developmental programmes have also been initiated for both ECRs and SL/Readers in research leadership.

EPMS has a forum of all ECRs (as defined by HR Excellence in Research), with two representatives on the School Research Committee. The forum promotes peer-to-peer interactions, interdisciplinary research and supports 'bottom-up' delivery of the Concordat. An important contribution comes from 'organic' activity within a multi-disciplinary School, buzzing with projects and many PhD students. There are reading groups, discussions, co-supervisions of PhDs by ECRs, workshops and collaborative events that all help to broaden experience, identify collaborators and build confidence. The CDT contributes strongly to our environment's vitality, through recruiting multi-disciplinary student cohorts, and engaging them in joint activities and in external engagement.

All staff have an annual Performance Development Review (PDR) with their corresponding HoD or his nominee. All staff are assisted in proposal writing and the development of impact-related research by the Director of Research, senior academics and RHUL's R&I. As a measure of our success, most new academics have obtained grant funding as PI within three years of their

appointments and all who have completed their probationary period have been promoted (Albrecht, Bernardini, Blasco-Alis, Hague, Jensen, Quaglia, Sgandurra, Tzameret, Wahlström).

Applications for promotion are handled separately via an anonymous process to avoid unconscious bias. Applicants may seek advice from colleagues or local advisor panels, but the decision to submit is theirs, although HoDs provide comments on the application in consultation with a departmental promotions panel comprised of senior members of diverse background. Staff are either encouraged to consider the possibility of applying for promotion or given advice in terms of what steps they should take to improve on the applicable promotion criteria. The criteria are clearly identified on a matrix that is used by the Academic-Staffing-and-Titles Committee (ASTC) for making decisions.

College sabbatical leave policy, managed at School level since 2019, allows for single term sabbaticals or build credit for a full year. Staff who serve three years as HoD receive an extra one-year entitlement, to compensate for the loss of research time. During the assessment period 20+ terms of sabbatical were granted, that have resulted in establishing new collaborations (e.g., Chockler, Kalnishkan, Zhiyuan Luo, Paccanaro, Shanahan, Wahlström), journal publications (e.g. Johnstone, Murphy, Scott, Tzameret, Watkins), publication of new books (e.g., Martin, Vovk, and Zhaohui Luo), and new research applications (e.g., Bernardini, Cid, Gutin, Kinder, Paterson).

All members of staff with at least 26 weeks service are eligible for flexible working according to College Policy. They may change their working hours, the required times to work, or work from home. The policy is built on principles of equality and also recognises that staffing levels must remain in line with Departmental and EPMS School expectations. In this period, 5 members of our staff are working flexibly, two 0.2FTE, two 0.5FTE and one 0.6FTE. Changing from full-time to part-time involves discussions with the line manager and HR, to jointly agree on the adjustment to the volume of teaching and administration, including the tasks themselves in order to be compatible with the work pattern. One recent example is Paccanaro, who transitioned to 0.5FTE in 2019, after which he became responsible for teaching only one module, is assisted by a colleague in his main administrative role and has half of the average project supervision load. Where possible, essential meetings are confined within 10:00-16:00h.

We support staff interchanges with industry, academia and the third sector (both ways), ensuring our research is informed by real world problems and is used in practical applications. We have 17 visiting professors 11 from industry and 6 from academia: Helen Balinsky (HP), David Cooper (Enitor Consulting), Lars Carlsson (Stena Line), Pitt Lim (St George's Hospital), Debi Ashenden (Portsmouth University), Steve Babbage (Vodafone), Henry Beker (Founder of Baltimore Technologies), Andrew Clark (Primary Key Associates Limited), Whitfield Diffie (Pioneer of Public Key Cryptography), Paul Dorey (CISO Confidential Ltd), Dieter Gollman (Technische Universitat Hamburg), Igor Muttik (Cyber Curio, McAfee Labs), David Naccache (Ecole Normale Supérieure), Fred Piper (ISG Founder, retired), Martin Sadler (Former VP of HP Labs), Richard Walton (Former Director of CESG), Monica Therese Whitty (University of New South Wales).

We also support interchanges in the form of PhD placements (12 p.a. in our current Cyber CDT). In addition, we offer an honorary scheme allowing our PhD graduates and postdocs to maintain research links with us, e.g., Zukov (Blackrock) and Zhdanov (Amazon) are honorary research associates.

2c. Supporting early career researchers

Research and research-led teaching are our culture's main pillars, which we use to have positive impact on the world. New academic recruits are assured that advancing their research is a top priority for them and for the College. This is made evident in a number of ways: funding support

for specialised equipment and participation in conferences, workshops and research meetings; ensuring that their academic mentor advises on matters that affect their work, from explaining admin procedures to taking a strategic view of their research goals; supporting the funding of PhD studentships within their first three years; and reducing workload in the first year. The ISG also has an ECR mentor (Quaglia) with a particular focus on female ECRs. We further encourage new staff to co-supervise PhD students (with more senior colleagues), including our CDT. We also provide career development training for PDRAs and we inform them of new opportunities, from staff vacancies to new grant awards.

A workload model takes into consideration variations of funding and teaching loads for research and teaching focused staff. Within the EPMS School, we have evaluated our key administrative tasks and rationalised them to optimise the time spent by academics on research. We have also welcomed College's new teaching-focused route and recruited several teaching focused lecturers and fellows to increase research time for research active staff.

We use meetings, workshops and seminars to maintain our strong research culture. We have very active seminar series in computer science and in information/cyber security, with a mix of internal speakers, academic visitors and guests, as well as government and industry experts. These are widely advertised and are frequented by staff, PDRAs and PhD students across the unit. We also have termly staff meetings and annual away days. These have been used to assimilate new academics and update everyone in the research themes. The spirit of cooperation inspired by these meetings has enabled us to generate new ideas and identify new collaborative research opportunities and strategy.

2d. Research students

We have increased the average number of PhD students entering p.a. from 17 in the previous period to about 29 in this period through a number of stimulating initiatives and complementary schemes: the Leverhulme CDT on 'Freedom and the Rights of the Individual in the Digital Age'; EPSRC CDTs in Information Security; supportive departmental scholarships and collaborative PhDs with industry (half-funded by companies and College).

Our large and diverse PhD community is a thriving source of energy and creativity, which although guided and nurtured by staff, provides a much greater return to them in terms of vitality and research output. Nowhere is this 'buzz' more evident than in the three consecutive EPSRC Cyber Security CDTs, in which every annual cohort (~10 students) contributes more than the sum of its parts. Across the whole CDT, the gender ratio is 40:60, women:men, but this figure reversed in the last cohort. The current CDT, 'Cybersecurity for the Everyday Life', which started in 2019, supports the sustainability of our PhD programme.

Recruitment: We typically respond to 150 formal applications (plus more informal enquiries), and from these we recruit between 25-35 PhD students each academic year. Most of the recruited students have a first-class degree or a Merit/Distinction at Masters level, while applicants with work experience are strongly encouraged to apply. Potential supervisors interview candidates based on their research proposals and applications. Upon arrival students attend induction meetings with their supervisory team, the Director of Graduate Studies (DoGS), and IT support. Induction ends with sessions delivered by the Graduate School, where students meet colleagues from other disciplines.

Support and monitoring: Students who join us are followed by a supervisory team consisting of a supervisor, possibly a co-supervisor and an advisor who has a pastoral role, and report quarterly to the DoGS. An annual review is based on a student's report and a presentation at the annual PhD Colloquium, held each summer and organised by the students. An upgrade meeting from

MPhil to PhD is held from the beginning of year 2 of study (year 3 in CDT). The supervisory team and an independent academic evaluate progress and a thesis plan, making their recommendation to Doctoral School, with oversight of the DoGS.

Students are provided a high-end computer and desk space in an open-plan space to which they have full 24h secure access. New CDT cohorts are co-located to maximise group dynamics and training exercises. There are multiple funding models for different types of PhD student, but generally the Department and/or project PI will ensure that students receive financial support for attendance at academic events provided they present peer-reviewed research. Depending on the research group, students may also obtain grant-funded resources, such as access to specialised equipment, lab access and additional travel. Where possible, students of the same research group are co-located.

Skills development and careers: Students attend researcher development programmes from RHUL's Doctoral School providing transferable skills (e.g. thesis writing or managing publication data), and more general skills aiding employability (e.g. effective presentation skills or managing work/life balance). The programme is structured using the Vitae Researcher Development Framework. Students also receive guidance on curriculum development and learning technology through inSTIL: a Programme in Skills of Teaching to Inspire Learning, a condition for participation in teaching activities. On top of this generic training, we provide subject-specific training on how to write scientific computing articles, present them in conferences and on preparation for PhD-vivas. We pay for 'Wednesday cakes', a student-run series of presentations that promotes scientific interaction.

All PhD students are expected to regularly attend departmental seminars. Industry seminars (e.g., Amazon, Blackrock, ASOS AI, PwC, Facebook) not only promote better understanding of industry needs, but are also career oriented, providing connections between employees and students. CDT students have an additional first year of training that involves lectures from industry and off-site visits. There is also opportunity to take placements with employers for on-the-job training. Industry placements are also available to non-CDT students, typically after their transfer to PhD. Of the 83 students graduating from the unit (Fig. 3), almost 60% went to industry in research departments of organisations such as Amazon, Blackrock, Cloudfare, Facebook, Globalsign, HP Inc, JP Morgan, Microsoft Research, Mozilla Foundation, Nomura, and Yahoo.

2e. Equality and diversity (E&D)

RHUL was one of the very first women Colleges founded (1886). The doors are now open to all, but the equality ethos is very much in our DNA. Regarded as one of the most international UK universities, we welcome students from over 100 countries. The College actively endorses the seven principles outlined in the Concordat to Support the Career Development of Researchers and has policies and practices designed to fully implement these principles, e.g. mandatory training for selection panel members including equal opportunities training; equitable treatment for part-time and fixed-term staff; and an equitable promotions process. Extensive development opportunities include a centrally administered mentoring programme (supplemented by departmental ECRs mentoring), which is open to all research staff, and a comprehensive annual equality and diversity data-monitoring and review exercise. The College has an institutional policy to narrow the gender pay gap by 2021 and a working group was established in 2018-19.

The School E&D Directorship is shared between ISG (Coles-Kemp) and Mathematics. The Athena SWAN Bronze was awarded to CS in 2013 and to ISG in 2020. Two Champions (Bernardini and Quaglia) chair E&D committees in CS and ISG respectively and manage a regular forum including E&D activities and external speakers. These committees meet termly to discuss and agree

departmental E&D initiatives. E&D issues are a standing item on the termly departmental board meetings. Since 2019, outputs from these fora feed into the EPMS School E&D committees, Research Committee and School Executive. E&D issues are embedded in a number of research and education activities. These include: a monthly E&D reading group for staff and students and a critical security reading group for staff and students. Diversity is further promoted through weekly ISG research seminars in research topics ranging from security of technology to security of underserved and vulnerable groups.

In this period, our staffing strategy has created a more inclusive environment from the last period in terms of FTEs (a) BAME staff increased from 7% to 14% and (b) female staff increased from 4% to 17%. An example of our E&D policy's success is Bernardini's trajectory in CS, appointed as lecturer in September 2015, promoted to SL in November 2017 and Professor in July 2019. In 2018, she was offered a sabbatical term to take up a visiting professorship at MIT. As a result of her excellent work in AI planning, she has been supported by CS and our R&I office with a number of successful Innovate UK research applications and was selected at School level to apply for the Turing AI Acceleration Fellowship.

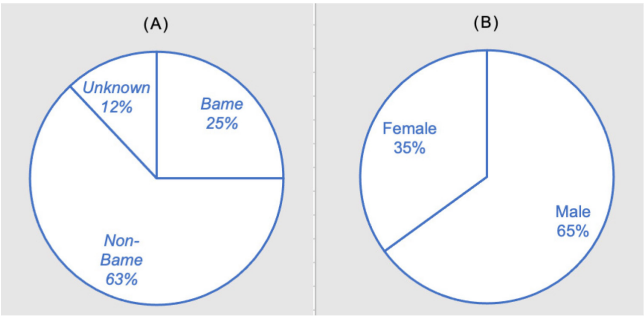

Figure 3: *Demographic of PhDs awarded in this period*

Fig. 3 shows how E&D policy is reflected on our PhD graduates. Overall, the number of women in our PhD population has also increased by 20% in this period, which leads us to mention the 'WISDOM' group, another E&D success. The group was founded in May 2016 by two women PhD students, who wanted to create an opportunity to raise the profile of women working in Mathematics and Information Security, to encourage more women into these disciplines. WISDOM has since expanded across all disciplines within the EPMS School, including Computer Science. It discusses E&D in its broadest sense. WISDOM offers a strong support network to students and staff, who are interested in equality and exploring ways that more women can enter and prosper within academia. WISDOM activities include monthly lunch meetings, workshops, discussion groups and outreach activities including socials. The group's achievements were recognised in 2017 with the Principal's award for enhancing fairness. Since then WISDOM has focused on individuals from under-represented backgrounds with emphasis on broadening the horizons and supporting career progression of researchers, raising their research profile within the EPMS School and undertaking outreach.

We also support members of staff returning after a period of absence (e.g. sick leave), by asking HoDs to allocate them duties that can be carried out as flexibly as possible. Moreover, support for staff with protected characteristics and equality and diversity issues affecting career progression are discussed and agreed as part of their PDR (section **2b**). Advice and guidance are being developed for the next PDR period to further support staff in raising such issues where appropriate at their PDR meetings. The School E&D Director has an open-door policy where staff can raise E&D issues or seek advice from the E&D Director as a further line of support.

We provide assistance before, during and after maternity or adoption leave. Besides flexibility in preparation arrangements, staff are provided resources that they may need during their leave, e.g.

a laptop, and the College has a policy encouraging staff on maternity or adoption leave to keep in touch with their Department. The EPMS School has a specific policy for academic staff returning from maternity of reducing the teaching and administration workload. Typically, this would include a full term without teaching or administration, to give returning staff time to catch up with research. Funds are also made available for equipment, travel to conferences, and research visits to (or from) collaborators.

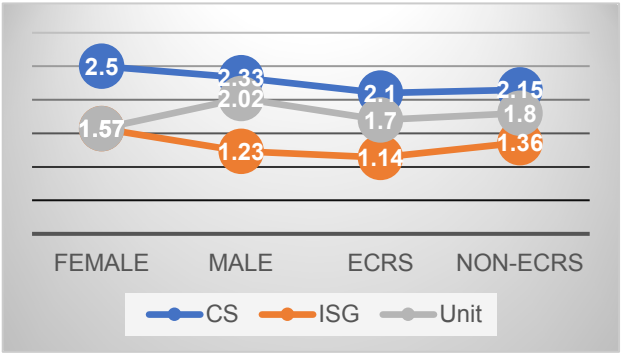

Figure 4: *Average output contributions*

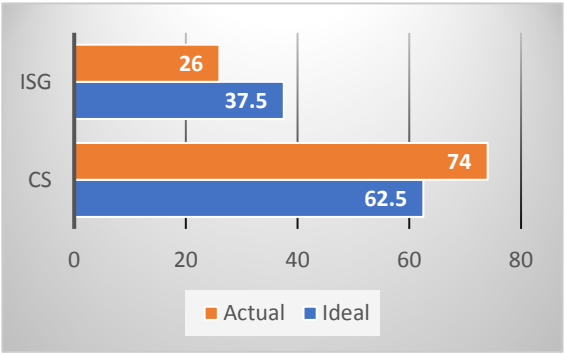

Figure 5: *Outputs by Department*

Equality and Diversity in the REF submission. E&D considerations have played a key role in our output portfolio selection (Figures 4 and 5). Based on the College Code of Practice, all members with research responsibility and assessed as independent researchers were asked to nominate five outputs since January 2014 with the potential to be assessed as internationally excellent. A unit REF Lead (CS), with a REF co-lead (ISG), and the two HoDs have overseen that a rigorous assessment of output quality has taken place. Assessment involved critical evaluation according to a shared set of criteria, and all proposed outputs have been assessed internally by two reviewers. Where no suitably qualified academic staff was available to undertake this, or there was an indecision around borderline outputs, we engaged a reviewer from another institution, approved by the Chair of the College REF Steering Group. Once a rating for the outputs was agreed, the REF team selected the highest rated outputs for submission. For equally graded outputs, we prioritised any imbalance identified in the most current Equality Impact Assessment.

3. Income, infrastructure and facilities

3a. Research income

As part of our strategy, we encourage our members to target a variety of grants, with the aim to diversify the support of our research activities from different bodies. During this period we have secured grants that have reinforced the increasing vitality of our research environment and have made our research portfolio more sustainable. Fig. 6 shows the increase in our research income (spend) from ~£7.42m in the last period to ~£13.2m in this period. This funding comes mainly from UKRI, industry and the EU; the total values of research grants from these bodies increased by 40%, 34% and 54% respectively. Our income from charities has risen by 70%. The overall research income in terms of grants awarded for this period has been ~£11.5M (~1.65M p.a.), with industry funding almost tripled since the last period. We have also complemented our grant income with ~£0.5m from consultancies.

A selection of successes contributing to the development and diversification of our research over the period are as follows. Three EPSRC CDTs have made a major impact on our research. Growth of AI and robotics with potential future impact (Bernardini) has been strongly supported by UK Innovate (£0.9M). Research on cryptography has been supported by £3.5M awards, including EU's Prometheus and FutureTPM. Socio-cultural aspects research has been boosted by £1.1M

EPSRC awards to Coles-Kemp, as well as the Leverhulme CDT in 'Freedom and the rights of the individual in the digital age'. Special unit events in joint areas of interest (e.g., cybersecurity and e-health) have fostered internal collaborations. Overall, from our 41 Category A staff, 30 have been investigators, 27 as PI.

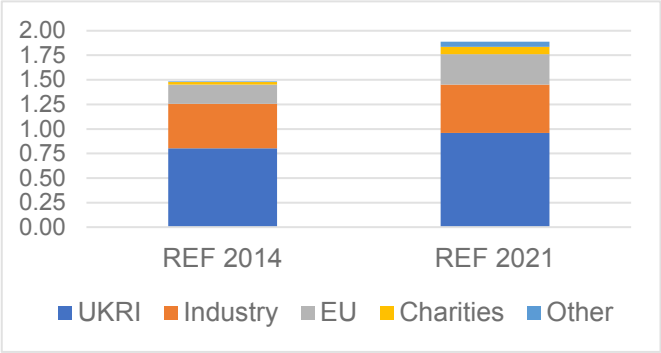

Figure 6: *Average annual spend by source (£M) in REF2014 and REF2021*

A brief summary of a selection of recently funded projects already impacting on strategy follows. In the Advanced Quantum Science and Technologies catalyst, ISG will continue with developing novel post-quantum algorithms for bridging the gap between lattice coding and lattice cryptography based on the new project by EPSRC EP/S02087X/1. The ISG will also build upon the Trusted Platform Modules project (EU-779391 FutureTPM, £321,794), for securing IoT systems within a post-quantum world. CS has been boosted by two recently awarded EPSRC projects: Hague (EP/T00021X/1, £393,618) will target regular expressions for programming languages used for internet applications; Sammartino (EP/S028641/1, £313,577) will target verification of software concurrency via model-learning. Research on algorithms and complexity has also received a further boost by the award of an ERC Consolidator grant to Tzameret in December 2020.

3b. Operational infrastructure

All our researchers have access to a dedicated computing infrastructure, which is supported by a technical team of four. This infrastructure provides access to a Virtual environment consisting of three HP BLADE servers, each server having resource of 32 CPUs 512GB RAM total resource or 96 CPUs and 1.5TB RAM, which is connected to a 10GB VLAN network. Alongside this, the infrastructure has several GPU servers running NVidia Tesla K40 GPU Computing Accelerator - 12GB and M60 8GB (GDDR5). A computer lab of 30 MSI trident desktop with GTX 1060 DDR5 6GB GPU, each connected to 1GB network with 10GB uplink. The entire infrastructure is behind a dedicated active/passive Firewall, provides data transfer over JANET and has a separate internet connection of 300MB. Regular audits of our buildings ensure they are accessible to anyone with a disability.

We also distribute infrastructure to individuals or groups, often in the form of small test and development units for microprocessors, FPGA, IoT, drones and robots. For ISG research, isolated equipment is sometimes necessary to prevent malware contamination, or loss of sensitive data; or to precisely control CPUs when detecting unintentional information leakage, or covert communication channels.

3c. Physical infrastructure

The unit is housed in the completely re-purposed and refurbished Bedford building, a prioritised investment of £5.9m. PhD students from CS, ISG and Mathematics are co-located, promoting interactions and interdisciplinarity. The building co-locates researchers whose expertise falls

within the two central technology pillars of the College's digital research catalyst: Artificial Intelligence/Machine Learning and Information/Cyber Security. It also serves as the administrative hub of the EPMS School.

We make full use of the further major infrastructural investment made by RHUL in this period, such as the Emily Wilding Davison library (£57 million). We used this fully accessible space for the '200 Years of Becoming Digital' exhibition to celebrate the 50 years of our CS Department. Bedford also provides us facilities for meetings, labs and workshops.

As hosting workshops and conferences is an important part of our scholarly life, College provides numerous quality spaces and campus accommodation for attendees. We also host events in RHUL's London base at Bedford Square and the UoL Senate House as part of our research operations. There we hold our Industry Advisory Board, PGR training events, including interdisciplinary consortia workshops (e.g. Techne AHRC DTP). Funding from Research and Innovation's budget and from CS/ISG is also available for all unit members to host and promote new projects, specialist workshops and public debates in other London locations (e.g., the prestigious BCS London and British Academy).

4. Collaboration and contribution to the research base, economy and society

4a. Collaboration, Networks and Partnerships

We develop and maintain a variety of strategic collaborations at local, national and international level, ranging from research networks to major projects underpinned by collaboration agreements. These enable us to maximise opportunities to develop the discipline and strengthen the impact of our research. We encourage open research supporting sharing, transparency and reproducibility, whether this is about papers, data and/or software (section **1h**).

RHUL, via the ISG is recognised by GCHQ/NCSC as an Academic Centre of Excellence in Cyber Security. In 2019, our ISG was pivotal in the establishment of the International Cybersecurity Centre of Excellence (INCS-CoE). The founding members of this Centre along with RHUL via the ISG (Cid, Sgandurra) are Keio and Kyushu Universities (Japan), the University of Maryland Baltimore County and Northeastern University (US) and Imperial College (UK). INCS-CoE has since spread to Australia and Israel, and Cambridge University has joined in the UK. It serves as a hub for international collaboration between academia, government and industry.

Our Computer Learning Research Centre has been carrying out pioneering work in statistical learning theory, conformal prediction (Gammerman & Vovk) and Q-Learning (Watkins). Recent work builds upon a series of international strategic collaborations, especially in the area of 'Compound Activity Prediction Engines' within the EXCAPE EU project (Gammerman, Zhiyuan Luo and Vovk), where a 'multi-target ML' framework is used for drug discovery. The novel techniques of this work are developed in collaboration with the Universities of Aalto (Finland), Linz (Austria) and Ostrava (Czech Republic) and industrial partners including Intel (Belgium).

Further collaborations of individual members are as follows. Albrecht with ETH Zurich (Post-quantum cryptography, EPSRC funded), Bernardini with MIT and Toronto (Autonomous planning, EPSRC funded), Cohen and Hague with Oxford (Constraint satisfaction and Push-Down Automata respectively, both EPSRC funded). Coles-Kemp with Imperial and Newcastle (security and safety of services, EPSRC funded), Gutin with University of Southern Denmark and separately Universities of Shaoxing, Nanjing and Nankai (Graph Theory, funded by EPSRC and the Danish and Chinese governments). Hague with Uppsala University and TU Kaiserslautern (concurrency verification, EPSRC funded), Johnstone and Scott with Swansea, Newcastle, Delft, CWI Amsterdam and TU Eindhoven (programming languages, EPSRC funded). Zhaohui Luo with

Toulouse and Gothenburg (type verification, EU funded). Paccanaro with Yale and Cornell (NSF and EPSRC funded) and Tzameret with Toronto, and Oxford (proof complexity, EU funded).

4b. Relationships with users and beneficiaries of our research and knowledge transfer

Our research touches diverse communities as well as general audiences, beyond the work captured in our impact case studies. Our ISG has long-standing relationships with HP Research Labs (Paterson) and Vodafone, spanning joint research, internships and PhD sponsorship. Moreover, collaboration with a variety of companies, e.g., BAE Systems, BT, Cloudflare and IBM, have allowed us to train over 90 PhD students in areas such as embedded security, cryptography, geopolitics of security, and cyber economics. Some collaborations involve interdisciplinary projects e.g., the work with GSK on 'Risky cyber-behaviour in organisations' (Jensen). GSK used the research programme to test the effectiveness of various interventions to increase cybersecurity.

Work on ML has already been taken up by AstraZeneca (Sweden) and Janssen (Spain). Similarly, recent work with British Gas and Centrica on 'Big data analytics' (Gammerman and Zhiyuan Luo) and with AlgoLabs on 'Trading strategies using on-line ML' (Kalnishkan and Watkins) are further examples illustrating our industrial links. Similarly, Chockler and O'Keefe collaborate closely with IBM on distributed and scalable infrastructures for trustworthy services. Bernardini maintains strong links with user organisations on autonomous systems, including NASA, the UK Atomic Energy Authority, and BAE systems.

We engage with general audiences in the History of Computing through the work of Johnstone and Scott on a steam-driven version of Babbage's Difference Engine. This shows how such an engine makes tables of mathematical functions that can be programmed to a limited extent and was broadcasted by the BBC2 documentary 'Monkman and Seagull's Genius Adventures' on 25 May 2020. The same Difference Engine was also exhibited during the 50 years celebration of our CS Department, linking the local community with our scientific heritage.

4c. Contribution to economy and society

Our impact case study for the security improvement of the TLS protocol is used by billions of people on a daily basis for secure web browsing (and more). As a direct consequence, major vendors including Apple, Google, Microsoft and Mozilla removed RC4 as an encryption option in their browsers, and the figure is now well below 1%. The global annual impact of this study on e-commerce alone has been estimated at several trillions of USD.

In another case study we provide algorithmic foundations for new distributed systems technology built by IBM in two key business areas: (a) a server platform facilitating management of applications hosted on the IBM cloud and (b) a generic permissioned blockchain facilitating secure management of critical assets (such as cryptocurrency) within an organisation's network relying on distributed ledger technology (DLT). Consequently, IBM increased DLT scalability significantly, which in turn, boosted its attractiveness for customers of large computing bases.

Our significant contribution to drug discovery is detailed in another impact case study and arose from the application of conformal and Venn predictors. These methods made a major contribution to reducing the time and costs involved in drug discovery at AstraZeneca and Janssen Pharmaceutical.

A key finding in our final impact case was that evasive and non-compliant cybersecurity practices are likely to result if technology is deploying a service people regard as not useful or damaging their wellbeing. With ~1,470 participants, the research produced 'creative securities', a

participatory method examining the intersections between risks to people and risks to technology. This work demonstrates how we have changed current cybersecurity policy and practice.

4d. Contribution to and recognition by research base

We regularly lead academic activities nationally and internationally, shaping agendas and strategies. Our research base contribution can be effectively measured by our involvement in editorial boards. Examples include Designs, Codes & Cryptography (Mitchell - Editor in Chief, Albrecht, Cid), AI Journal - Elsevier (Cohen), Journal of ML Research (Watkins), Nature Scientific Reports (Paccanaro), Discrete Optimization (Gutin), Order (Gutin), Memetic Computing (Gutin), Journal of Computer Languages – Elsevier (Scott), SN Computer Science (Gutin), Ambient Computing and Intelligence (Stathis), Cybersecurity Journal - Springer (Cid), IACR Transactions on Symmetric Cryptology (Cid), Data Science Journal (Shanahan), Information Processing Letters - Elsevier (Chockler), Information Management and Computer Security (Coles-Kemp), Journal of Cybersecurity - Oxford Academic (Coles-Kemp), Electronic Proceedings in Theoretical Computer Science (Fiadeiro), IET Cyber-systems and Robotics (Zhiyuan Luo), The Computer Journal (Martin, Mitchell, Sgandurra).

Academic leadership is evident in our service to conferences and workshops. On average, each academic is in committees of 2-4 international conferences p.a. Our leadership here includes:

- **Keynotes** – We gave over 70 invited presentations and keynotes in national and international events. Examples of keynotes include Tzameret: CSL'20; Gutin: TAMC'20; Vovk: ISIPTA'19; Albrecht: AFRICACRYPT'19; Cid: IWSEC'19 (M&IS session); Stathis: ICDSST'18, JFSMA'18; Chockler: BTT'17; Mitchell: ACISP'16; Paccanaro: FEBS'16; Martin: CECC'15, ICCC'15; Quaglia: TRUST'15; Shanahan: CLOUDTECH'15; Zhaohui Luo: LACL'14.
- **Conference chairs** – We served in the organising committees of over 50 conferences/workshops. Examples as Program or General Chair (GC) include Albrecht: IMA CCC'19, QuAC'19; Bernardini: InteX'17, SPARK'19; Cid: SAC'18 (GC), FSE'14; Chockler: P2P'14 (GC), LADIS'18, CCGRID'20; Fiadeiro: WADT'18 (GC); Gammerman: COPA'15-19; Hague: HOPA'14-15, INFINITY'16, HIGHLIGHTS'17, BCTCS'18 (GC); Zhiyuan Luo: SLDS'15; Mitchell: SSR'14&16, ISC'15, STM'17, ICICS'17; O'Keefe: RaSTEES'19; Paoletti: CMSB'16, VEMDB'18, HSB'19; Quaglia: WCS'17, Crossfyre'18; Scott: Parsing@SLE'16; Sgandurra: CYSARM'19; Stathis: AMI'18; Vovk: COPA'14 and GTP'14 (GC).

We received prestigious awards and participated in review panels, advisory and policy shaping boards. Gutin is Member of Academia Europea and recipient of the Royal Society Wolfson Research Merit Award. Wahlström was awarded the 2018 Nerode Prize. Cohen, Johnstone, Martin, Scott and Stathis are BCS Fellows, while Cohen, Coles-Kemp, Johnstone, Hague, Zhaohui Luo, and Watkins EPSRC College members. Paccanaro is BBSRC expert and advisor to the Paraguayan Government. Our members regularly evaluate research from international funders e.g. China's NNSF, Canada's NSERC, EU's (ESF, ERC), Israel's ISF, Norway's NWO, and Poland's FNP. Chockler and Mitchell acted as senior consultants, the former to IBM Haifa on Cryptocurrency and the latter to Huawei UK on Security. Coles-Kemp has been a member of DCMS advisory panel for the code of practice on Consumer IoT security, and deputy director of the Research Institute for the Science of Cyber-Security.