Institution: Royal Holloway, University of London
Unit of Assessment: B10 Mathematical Sciences

a. Context

Royal Holloway has a strong and continuing tradition of mathematical research aimed at impact, going back to work on cryptography from the mid-1980s and the formation of the Information Security Group (ISG) in 1990. The increasing importance of information security led to a rapid expansion of the ISG within the Department of Mathematics, culminating in the formation of the School of Mathematics and Information Security in 2012, comprising the Department of Mathematics (DoM) and the ISG as equal partners. As one might expect given its ancestry, the School has a unified approach to research in general and impact in particular, with its research committee, Director of Research and Impact Officer having School-wide remits. Moreover, the boundaries between the DoM and the ISG are fluid, with members of the ISG being submitted to UoA B10 (the majority of the ISG submission falls under UoA B11), and members of the DoM collaborating and co-supervising PhD students with members of the ISG. The approach to impact is coordinated across both units, involving similar structures and shared activities. Members of the UoA B10 submission are involved with all activities mentioned here.

Current non-academic beneficiaries of mathematical research in the School include: users, manufacturers and distributors of information and communication technology relying on results of discrete mathematics and cryptography; GCHQ and all users profiting from research enabled by departmental links with GCHQ; those involved with our programme of public engagement activities. These groups benefit from the economic and societal advantages arising from connecting digital devices more securely, not least the increased trust in e-commerce, e-government and mobile telecommunications and the consequent advances in public policy and practice.

b. Approach to impact

The School continues its long-standing tradition (originating with the formation of our cryptography group in the mid-80s) of applying mathematics to industrial problems, and strong public engagement. Our long-term and successful approach is to encourage direct links with industry so as to understand the real-world issues in depth, before using our research skills to solve any resulting problems. In 2012 Royal Holloway was awarded the status of an Academic Centre of Excellence in Cyber Security by EPSRC and GCHQ, in recognition of the success of our work in information security in particular. Several mechanisms are used to encourage industrial links:

(a) **Consultancy and secondment** is encouraged. Cryptographic consultancy in the School is performed either by standard institution consultancy supported by Royal Holloway’s Research and Enterprise Office (which negotiates contracts, sets up budgets and processes payments), or in tandem with Codes and Ciphers, a consultancy company specialising in information security whose Director, Fred Piper, is an emeritus mathematics professor at Royal Holloway. Consultancy has included the design and analysis of ciphers and wider protocols for banks, telecommunications companies and others. Other examples of consultancy range from an annual arrangement with the Heilbronn Institute (2 staff members; up to 60 days per year in total) to a short (1 day) project (Blackburn) using design theory to construct golf tournaments. Staff undertaking consultancy can opt to be paid additional salary, and are given increased budgets for research or industrial outreach activities. Secondment is encouraged: a recent one-year secondment to the Heilbronn Institute has had confidential impact in the current REF period.

(b) **Networking at conferences** attended by representatives from industry (often growing naturally from our applied research). To supplement this, Blackburn is a Working Group chair for an EU COST Network in Network Coding, which provides funds to speak at events with co-speakers from (for example) Telecom ParisTech and the European Space Agency.

(c) Encouraging **PhD projects with potential impact; training PhD students** for the marketplace. Recent supervisors and relevant PhD projects include Schack (2008- ; security models involving quantum players), Ng (2008- ; authentication in vehicular ad hoc networks) and Blackburn/Cid (2008-11; group-based cryptography). EPSRC CASE studentships (with GCHQ as the industrial partner) have been obtained by Blackburn (2013-) and McKee (2008-12). PhD students trained in the Department who use technical skills gained here include: Richard Horne, Managing Director, Cyber Security, Barclays; Karl Brincat, Head of Technology Risk, Visa Europe; Simon Blake-Wilson, Vice President of AuthenTec's Embedded Security Solutions. Royal Holloway is a **Centre for Doctoral Training (CDT) in Cyber Security**; Blackburn is supervising one of first generation of ten CDT students, who arrived in October 2013.

(d) **Research projects and grant applications** aiming directly at impact. Examples taking place, or having impact, within the current REF period include: Koloydenko's statistical work (2007-) on a diagnostic tool using Raman Spectroscopy for improving skin cancer treatment; EPSRC grants (Blackburn, co-PI) on the combinatorics of wireless sensor networks and follow-on work by Blackburn and Gerke; work (Cid, Murphy, Robshaw) that sets the security of the Advanced Encryption Standard (AES) in a proper algebraic framework, and subsequent related EPSRC grants. These activities form part of a wider group of interdisciplinary projects within the School that touch on mathematical topics (Paterson’s work bridging theory and practice in cryptography, and Wolthusen’s work on graph-based models in the Internet of Energy are examples here.)

(e) **Public engagement** (in applied maths, coding theory, cryptography and pure maths) aimed at the wider community. This includes: involvement with the Headstart programme (a national residential STEM outreach programme; 60 school students per year visiting the Department), Exploring Maths (a one-day on-campus event for 6th formers; 400 students); maths events in the Royal Holloway Science Festival and Open Day (over 2500 attendees each year); the annual Coulter McDowell public interest lecture (400 attendees); a programme of school talks (approximately one visit per month); lectures at the Café Scientifique (Croydon); assorted radio and TV interviews (examples since 2008 include appearances on The One Show (BBC) and Teachers TV, radio interviews with CNN America, BBC local radio stations, and CBC Radio Canada). These activities are supported by the institution’s Communications and Press Office. In addition to this work, Royal Holloway hosts meetings of the Further Maths Network, and we are the host department for Gillian Burke, the Coordinator for the Network covering the Southern Counties.

(f) The School organizes and participates in several major **industry-focussed meetings** on campus per year to maintain and strengthen our industrial links:

- The annual one-day **Hewlett-Packard Colloquium on Information Security** (over 100 participants; 75% from outside academia). Three one-hour talks are given, with at least two (often all three) speakers from industry. Recent speakers include representatives from Cisco Systems; Downtown Associates (an information security and privacy consultancy); ETH Zurich; Sophos (antivirus); Verisign/iDefense (internet infrastructure and security); Verizon Enterprise Solutions (networks and mobile technologies). Hewlett-Packard and Royal Holloway research demonstrations and posters are presented, and ample networking opportunities are provided.
- The annual **Smart Card Centre Open Day** (over 100 participants; 75% from outside academia). The event consists of two exhibition sessions, with exhibitors from industry together with Royal Holloway MSc and PhD student exhibitors, followed by a one-hour talk. Networking takes place over coffee and lunch, as well as during the exhibition sessions. In 2012, for example, exhibitors from the smart card industry included Orange Labs (UK); UK Cards Association; Transport for London; ITSO; Collis; Comprion; Cubic; Barnes International; Oberthur; Gemalto; MULTOS; Crisp Telecom; Incoming Thought; ARM; IISP.
- The twice-annual **Networking Dinners** (approximately 65 participants; 85% are from outside academia). Each event consists of a drinks reception followed by a meal. Representatives from across the information security industries attend, for example representatives from: BT, CESG, Deloitte, KPMG, Nationwide Building Society, Royal Mail Group, Thales, Unisys and Visa**.**

c. Strategy and plans

The impact agenda is embedded in the School’s strategy in several ways.

(a) **Staffing**. When making academic staff appointments, the School aims to maintain a balance between its different research areas. This includes a balance between research areas that are likely to lead rapidly to impact and those with a longer-term, underpinning role. The recent (non-replacement) appointment of a statistician (Shcherbakov) demonstrates the School’s commitment to developing research with strong impact potential.

(b) **Continued close research collaboration between the Maths Department and the ISG**. Mathematics with high potential for impact is most likely to be generated when mathematicians have a good appreciation of the problems and techniques of more applicable fields. Close research collaboration is an important way of nurturing this appreciation. The impact of information security as a research area has been recognized through recent government initiatives relating to cyber security: the School’s applicable mathematicians were a key part of Royal Holloway’s successful ISG-led application to become a GCHQ/RCUK Academic Centre of Excellence in Cyber Security

Research (ACE-CSR) (an initiative with a specific goal of building bridges between academia, industry and government). To maintain strong links between mathematicians and these areas of impact, we will continue to run **research seminars and study groups** involving UoA B10 topics attended by staff across the School, including the weekly Pure Maths and ISG Seminars (the latter often having speakers from industry), the PostCrypt discussion group (recent cryptography papers); and specialist groups such as the lattice-based cryptography group. These links will continue to generate **research projects** on UoA B10 topics with potential for impact, with future and ongoing projects such as linking probabilistic graph theory with adversary detection in networks (Gerke/Wolthusen), and using combinatorial techniques in network coding (Blackburn).

(c) **Supervision and/or co-supervision of PhD theses** with security-relevant topics, including CDT studentships. Examples include Blackburn, Ng (Discrete Mathematics) and Schack (Quantum Dynamics). The CDT in Cyber Security Research embraces UoA B10 topics, and benefits from the advice of the CDT's **advisory panel**, including industrial members from Barclays and BT and a Chairman Emeritus of the Institute of Information Security Professionals**.** CDT PhD students undergo 3-month industrial internships at such companies as IBM, McAfee, Thales, Vodafone and Logica, further cementing our links with industry and facilitating projects with genuine impact.

(d) **Networking** with industry via existing pathways, via the **CDT Showcase** (a conference to raise the profile of research from the CDT) and the **ACE-CSR Conference** (a two-day forum to share cyber-security knowledge across industry and academia and to identify research challenges).

(e) Recognition of the impact agenda in the **workload model**. The School workload model treats impact-related activities such as consulting on the same footing as research. Consulting is being encouraged actively. For instance, the School has given permission to two staff members to consult for the Heilbronn Institute for up to 30 days per year each.

(f) **Incentivisation**. Impact is discussed in, and encouraged via, the School's annual appraisal process. Impact is an important promotion criterion, and is one of the four main criteria that decide professorial salary.

(g) Support for **secondments to industry**. There have been discussions, for example, about a secondment within the next REF period, following on from the successful 2005/6 secondment to the Heilbronn Institute. The School welcomes such initiatives, and maintains a flexible approach to these (for example, helping with the logistics by rescheduling sabbatical leave).

(h) **Direct strategic support** for research with impact potential. For instance, in 2010 the Department allocated the only available fully-funded Royal Holloway studentship to Koloydenko in statistics, to support research projects on improved treatments for skin cancer. Similar future initiatives will be supported.

(i) Research/outreach funding as a **reward for consultancy activity**. A large proportion of consultancy income is made available to the academic for their own use, for example to fund further research projects or industrial outreach**.**

(j) The School has created the role of **Impact Officer**, to maximise the impact of the School's research, to promote the impact culture within the School, and to liaise with the Director of Research, the School's Research Committee and individuals (inside and outside the School).

(k) Strengthening our **public engagement** activities. Planned initiatives include providing Year 3 materials on mathematical topics to school teachers, with associated on-campus training.

(l) The Department will continue to make appropriate use of the institution's **support services and funding**, such as the Research and Enterprise Office (contracts, payments); the Research Strategy Fund (support for large grant applications and early career networking); Gateway and Park funds (for commercialisation projects); matched funded PhD scholarships (for part-industrially funded PhD projects); other departments' Impact Officers; staff training (all staff have the opportunity of attending impact training); and the Communications and Press Office (PR and support for outreach).

d. Relationship to case studies

Both Case Studies exemplify the School's approach to impact. Royal Holloway's design of algorithms underpinning the security of the TETRA standard (a worldwide two-way radio standard widely used by the emergency services) was a direct consequence of the School's close contacts with industry. Similarly, the School's long history of reliable consultancy and strong reputation in industry circles resulted in several mobile operators commissioning the group to redesign the authentication algorithm used in many GSM phones, the basis of our second Case Study.