CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

Spring 2019

CDT update

Director Report: Professor Keith Martin

The EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway has been awarded new funding for a further five intakes of ten PhD researchers from September 2019. This is fantastic news, and a testament to the efforts of everyone who has supported the CDT since it launched in 2013. I would like to particularly thank all those who contributed to the new funding bid through strategy discussions, proposal writing and provision of generous partner support letters. CDT recruitment for 2019 has now opened, so please pass on the good news and direct future cyber security PhD researchers our way.

One CDT or two?

With the new funding comes an important change to the CDT. While we have always welcomed multidisciplinary research projects, going forward there is a stronger emphasis on this. This is reflected in a new title: the EPSRC Centre for Doctoral Training in Cyber Security for the Everyday. Lizzie Coles-Kemp and Rikke Bjerg Jensen, who have both joined the CDT Management Committee to help facilitate this change, explain our new research focus in this newsletter.

This represents an evolution, not a revolution. We have a slight change to the management and governance teams, a refinement of our approach to recruitment, and a redesign of the first-year training programme. However, it does not create two different CDTs. The most significant change will be an increase in the breadth of diversity of cyber security research conducted within the CDT.

Departures and arrivals

I would like to extend my thanks to CDT Management Committee members Kenny Paterson and Johannes Kinder, who have both recently left Royal Holloway. Kenny was one of the architects of the CDT and has supervised a number of outstanding CDT projects. Arguably his greatest contribution was through his powerful research connections, bringing in many of the leading technology companies as CDT partners and facilitating valuable internship opportunities for CDT students, including in Silicon Valley. Johannes served as the CDT's contact within Computer Science, and was an enthusiastic supporter and promoter of the CDT within that community. Kenny has joined ETH Zurich, while Johannes has joined Bundeswehr University Munich, so you can expect to read about future CDT student visits to those parts of the world!

We welcome Martin Albrecht and Dan O'Keeffe, who have recently joined the CDT Management Committee, bringing their own networks and expertise to help steer the CDT in new directions.

Existing CDT cohorts

New funding is very exciting, but there is an existing CDT to run! The September 2018 cohort seem to be thriving, with a wonderful blend of personalities and skills. At the other end, we are now enjoying a steady stream of PhD vivas and completions. Two outcomes particularly mark the relentless march of time for me. Our original CDT funding was a product of the first UK National Cyber Security Strategy – now one of our CDT graduates has been helping to shape the next version of this strategy. Our development of our CDT was heavily influenced by our expert Advisory Panel – now one of our CDT graduates has joined that panel and is influencing the CDT's future direction. More details on the activities of current CDT researchers can be found elsewhere in this newsletter.

Diversity

Finally, an important observation. I think one of the greatest features of the CDT approach to PhD training is the bringing together of cohorts of diverse researchers, where diversity can be in terms of academic background, research discipline, age, gender, ethnicity, professional experience, etc. Of course, such diversity brings challenges and it requires everyone to be sensitive to these challenges. More than this, however, diversity provides opportunities. As we progress with what will, inevitably, be a more diverse CDT, it is through a respect for diversity in all its forms, and by everyone involved in the CDT, that I believe these opportunities can be seized and great research outcomes will emerge.

Inside the cohort

Jodie Knapp – 2018 Cohort

I have just passed the six-month mark of my first year within the CDT, and, upon reflection, it has been a whirlwind. Initially it took me some time to adapt to the shift in learning style, from my Mathematics degree being completely taught, to, now, being in a more academic setting. I felt overwhelmed with the sheer number of topics that I wanted to understand completely but did not always have enough time to do so. However, I have since learnt that I am not required to know everything at once, and, slowly, I have developed my knowledge base and skill set to prepare for my ensuing summer project. Despite the task being daunting, I see it as an opportunity to explore my interests more deeply, and practice researching and writing academically.Alongside my independent and taught studies, my cohort and I have plenty of training opportunities, reading groups, seminars, and support from other academics. I had a clear vision of how my first year would play out, however, to date, it has exceeded my expectations. A large part of this is due to my fantastic cohort. We are quite a large group compared to previous years, but I couldn't be happier with who I have been sharing this experience with and will continue to do so. Being together has only helped to create a more collaborative environment within which to work and support one another. Extending this to the wider CDT, everyone has been incredibly welcoming and helpful. This has made me feel very settled and I can only imagine it will benefit my path to PhD completion.

Jordy Gennissen – 2017 Cohort

I am now in my second year of the CDT, after completing a full year of training in a cohort represented by people from various disciplines, including international relations, mathematics, geopolitics, psychology, computer science and management. Because of this multi-disciplinary approach, we were, and continue to be, exposed to topics beyond our own, whether in training sessions or other events, such as when we played Andreas' cyber wargame (who passed his viva recently: congratulations!).

It can sometimes be difficult to keep up with each other's research. Yet, this does not stop us from putting effort into trying to do so through research seminars, PhD tea talks and social events.

The first year has encouraged many of us to learn more about areas of security different from our own backgrounds and this also influences the way we perceive our own research. As one fellow CDT student states: "The more you think about it, the more you realise how much the CDT's interdisciplinary approach actually shapes your PhD research - and its impact". Personally, I am currently reading up on cybercrime research in my spare time, despite this not being my core research area.

Reflection on Internships

Amit Deo

I recently returned from a three-month internship at the joint NUS/Singtel research lab in Singapore, where I was investigating alternative solutions to a secure data sharing problem that the lab has been looking at. Finding a satisfactory balance between functionality/efficiency requirements for certain parties and security in the presence of collusion was a particularly challenging aspect of the research. Despite the fact that I was working on a cryptography project, this internship gave me ample opportunity to learn about numerous techniques used in secure multiparty computation as well as the data structures that are used in the design of various schemes.

In my time there it was interesting to see how the interaction between the industrial and academic sides of the lab helped shape a common direction for the research being carried out. In particular, it was fascinating to watch presentations where representatives from Singtel would give feedback on the progress of research projects and identify possible future directions. It was very refreshing to see how inclusive the lab was in terms of allowing interns to attend such talks and showing a willingness for engaging in open discussion on research ideas. In summary, I am extremely grateful for the opportunity to visit the NUS/Singtel lab and for the opportunity to make useful contacts there. I am also thankful to both the NUS/Singtel lab and the CDT for making this internship possible.

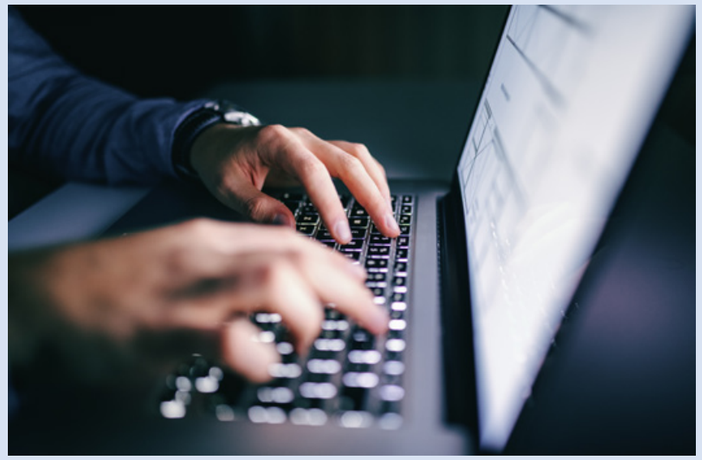
Research visits

Ben Curtis

One of the many opportunities supplied by our CDT is the ability to visit other research institutions in order to collaborate on projects. Research visits are typically set-up by an academic from your home institution through a known contact (such as a another academic or student working in the same area), but they can also be set up by the student themselves.

A visit to another institution can be a beneficial experience for several reasons. First, collaborating with other PhD students and/or academics allows for an academic network to be built or expanded, and also allows you to share knowledge with your peers. Second, learning how other people carry out research can allow you to develop new skills and therefore improve the efficiency of your own research. Third, such a visit can lead to a lasting research partnership, which is valuable for all parties.

Throughout the course of my PhD, I have been lucky to go on two such visits: the first in 2017 to TU Darmstadt in Germany and the second in 2019 to New Jersey Institute of Technology in the USA. Although both trips were only around ten days long (sometimes visits can be much longer, such as a few months), these research visits have been an invaluable experience and have helped to develop my research skills.



At Darmstadt I was visiting Dr Thomas Wunderer (who was then a PhD student, and has now graduated from Prof Johannes Buchmann's group). Dr Wunderer specialises in lattice-based cryptanalysis, and I was able to learn a lot during the course of this trip – much of which has set me up for future research. It gave me the opportunity to visit Germany for the first time and also allowed me to work alongside a more experienced PhD student, which is definitely beneficial for fairly new students.

At New Jersey Institute of Technology I was visiting Prof Kurt Rohloff, the Director of NJIT's Cybersecurity Research Center. This trip has resulted in an ongoing research project between Royal Holloway and NJIT. I was able to visit the offices of a start-up called Duality Technologies, who are based at NJIT, and are a company specialising in privacy-preserving computing through the use of, for example, homomorphic encryption. I will be going back to Duality in the summer as an intern, an exciting opportunity!

I would encourage all other students in the CDT who are interested in research visits to pursue this opportunity, and try to set up a visit to another institution – they are definitely worthwhile experiences.

New CDT in Cyber Security for the Everyday: a multi-disciplinary perspective
Lizzie Coles-Kemp and Rikke Bjerg Jensen

Since the turn of the 21st Century, the subject of information security has experienced growing diversification both at a practice (industry and government) and at an academic level. This move towards increased diversity is reflected in the funding calls, the interests of our MSc and PhD students and in the research challenges presented by many of our key stakeholders. Whilst information security still maintains a strong information and technology protection focus, this now sits alongside a broader mission of securing people, technology and society in a digital world. This process of extending both the scope of, and the approach to, our research and teaching, whilst upholding a strong connection with our data and technology protection roots, is illustrated particularly clearly in the story of our CDT in Cyber Security.

This year, with our first CDT having just taken its final cohort, we were delighted to be successful in the latest round of funding for UKRI centres for doctoral training. With this new award, we are able to launch a CDT in Cyber Security for the Everyday, with the first cohort due to start in September 2019. This is a truly multi-disciplinary initiative that brings together students from the mathematical sciences with those from the social sciences and humanities, by focusing on two main challenges:

- Security of emerging technologies, which addresses the security research challenges presented by technological evolution.
- Securing cyber societies, which addresses the security research challenges that emerge from increasingly connected societies.

In bringing these two challenge areas into one CDT, we are developing the ISG's tradition of high quality research in technology and data protection as well as demonstrating our ability to lead emergent research in the securing of people, communities and society at large in a world that is becoming more connected and increasingly digital.

The success of this CDT application lay, in part, in our ability to build upon on-going, successful supervisory partnerships with colleagues from a wide range of disciplines and departments across Royal Holloway. Our previous CDT established strong connections with Computer Science, Geography, Psychology and the School of Law. At the same time, the ISG was also involved in the Leverhulme funded Doctoral Training Centre (DTC) on 'Freedoms and the Rights of the Individual in a Digital Age' where, in addition to working with our CDT collaborators, we developed supervisory partnerships with Media Arts, Politics and International Relations and Classics. In envisioning and developing the CDT in Cyber Security for the Everyday, we combined these two supervisory networks with the broader supervisory capacity of the ISG. We did so to establish a foundation upon which a spectrum of PhD studies ranging from single-discipline studies that have an appreciation of wider disciplinary positions to the fully multi-disciplinary can be encouraged and supported. Establishing successful supervisory teams for this new CDT therefore builds on cross-departmental conversations and collaborations, as well as on the existing knowledge and experience held within the ISG.

Such a broad network produces diverse supervisory teams and challenges the way we navigate and undertake PhD supervision. From our experience with existing multi-disciplinary supervisory teams we have learned that these work best when they start from a shared and clearly expressed goal for the PhD study that is also shared by the student. This therefore also necessitates continuous conversations about disciplinary positions and methodological approaches throughout the PhD. Whilst each supervisor and the student will typically bring very different strengths, skills and knowledge to the PhD study, it is important that each contribution clearly supports the shared goal and values the different disciplinary perspectives

A multi-disciplinary PhD offers student and supervisors alike with the opportunity of a new and exciting study, but it can also be risky as there is no well-trodden path stretching out before the team. As such, supervisors must construct safe and supportive spaces in which not only students but also supervisors can experiment with new knowledge, work with different and sometimes conflicting bodies of literature and theory and explore new methods of research. Ideally, a multi-disciplinary PhD should result in a collaborative and rewarding learning experience for all involved. This is reinforced through a network of supervisory support mechanisms, such as workshops, courses and training sessions facilitated through the CDT.

In our new CDT, we are looking forward to welcoming additional colleagues into our network and establishing new supervisory teams. Not only shall we be working further on our approaches to multi-disciplinary PhD supervision but also learning from each other and our student cohorts as to what security education and training is needed for this type of multi-disciplinary programme. This is important so that the new CDT becomes a space that supports a wide spectrum of multi-disciplinarity; from single-disciplinary approaches with an appreciation for wider disciplinary positions to fully interdisciplinary PhD studies. Hence, a multi-disciplinary approach to PhD supervision, whilst not replacing the more traditional approach, extends and broadens the ways in which cyber security is researched and taught. The research challenges posed by the march of digitalisation require us all, whether student or supervisor, to reflect, respond and renew our research approaches and skills to successfully respond to the emerging cyber security research challenges enmesh themselves in everyday life.

During the long, hot summer of 2018, we had the pleasure of seeing four students from our first CDT cohort graduate with their PhD. Since then, it's been a steady flow of thesis submissions and vivas, and we're thrilled that all ten of our first-cohort students, along with four from the second cohort, have now submitted and have either been awarded or are (eagerly!) awaiting their viva.

The aim of the CDT has always been to deliver multidisciplinary researchers able to make a real impact within the fast moving world of cyber security. It is testament to the hard work and dedication of each of them that we now see them pursuing their careers in a variety of settings - including academia, industry and start-ups, each forging their own path in this challenging landscape.

In this newsletter, three students outline their CDT journey. We would like to take this opportunity to congratulate all completing students on their successful PhDs. We look forward to celebrating alongside each of them in the summer graduation ceremony this year!

Congratulations to: Dusan Repel, Jonathan Hoyland, Naomi Farley , Pip Thornton, Robert Lee, Steven Hersee, Alex Davidson, Andreas Haggman, Carlton Shepherd, Giovanni Cherubin.

Dr Pip Thornton – 2013 Cohort

This was not my intended thesis...

When I started in 2013, my proposed thesis was about military geographies. Influenced both by my time as a police officer in London, and by a brief but unsettling deployment to Iraq as a reservist soldier in 2003, I wanted to research how the military is represented in different physical, cultural and online spaces – specifically when away from the actual field of battle. Framing this proposal as a security issue was not difficult, especially as all things 'cyberwar' were particularly hot that year.

My first-year summer project changed all that. I'd been at a briefing at the Royal United Services Institute on the national and military security risk posed by the friends and family of service personnel posting compromising information on social media. Which was fine, except the phrase that kept being used was not 'friends and family', but 'wives and girlfriends', which not only erroneously gendered the problem, but also added derogatory cultural baggage relating to 'WAGs' and footballers' wives. This really annoyed me, so I went away to research the sexist connotations of the term only to discover that it was impossible to search for examples of 'wives and girlfriends' being used in a 'sexist' way, as the Google search engine automatically changed the word 'sexist' to 'sexiest'. So instead of feminist cultural critique, my 'wives and girlfriends sexist' query returned a list of the 'hottest' and 'sexiest' footballer's wives and links to 'lads magazines'. From that moment I became fascinated with how language is manipulated as it passes through the search engine, be that algorithmically, or by the processes of linguistic capitalism which govern Google's revenue generating advertising platforms. Luckily for me, both my supervisors – Pete Adey in Geography, and Keith Martin in the ISG – agreed that I could completely change the topic of my thesis and that they would still supervise me.

So my thesis was reborn as an enquiry into the linguistic, political, and economic side-effects of Google's search and advertising platforms, with the Walter Benjamin inspired title 'Language in the Age of Algorithmic Reproduction'. It was still about geography, as it focussed on the circulation of monetised language around the web, and on the location specific 'value' of words in different markets. And it was also about cybersecurity – not in a key-exchange and crypto way

(although there is a small amount of crypto in the project) – but because it exposed how the ability to access information, and to communicate across digital spaces is compromised by the manipulation and exploitation of the language that flows through them.

This switch to a topic with language at its heart was also particularly interesting for me because it necessitated a return to my academic home in English Literature and critical theory such as post-structuralism. I began to think of ways to make visible (and explain to my funders) some of the ideas I was having around Google and language, and a very effective way of doing this was through the medium of poetry. To begin with, I worked out the monetary value of the words of a well-known poem as they would appear as keywords in a Google search advert and presented the results as a mocked-up receipt to demonstrate the tension between the 'poetic' and 'economic' value of language in an age of algorithmic reproduction. The word 'cloud', from William Wordsworth's 'Daffodils', for example, has a high monetary value to Google, however its value lies not in a vision of a Cumbrian springtime, but in the context of 'cloud' computing and associated technologies. The poem receipt provided a means for me to expose the inherent structural and market logics which almost invisibly govern the words that flow through the search engine. As time went by, and with the help of fellow CDT students, in particular Ben Curtis and Feargus Pendlebury, the poem-receipt process was semi-automated to process longer texts, I bought a second hand receipt printer to print out and frame physical receipts as artefacts, and the project became a fully-fledged artistic intervention called {poem}.py.

Daffodils
by William Wordsworth

SALE

30th Sep 2017 10:00PM
BATCH #: CRC32
AUTH #: 3478199467
AREA #: ALL

1	i	£0.72
1	wandered	£0.49
1	lonely	£0.57
1	as	£0.20
1	a	£0.31
1	cloud	£3.01
	SUBTOTAL	£5.30
	TAX:	N/A
	TOTAL	£5.30

APPROVED

Thank you for shopping at Google

CUSTOMER COPY

{poem}.py

Since then, I have presented my work at a range of national and international venues such as the Science Museum, the Alan Turing Institute, New Media Scotland, and the Transmediale festival of art and digital culture and {poem}.py has gone from strength to strength. The project was covered by WIRED UK and New Scientist in 2018, and a collection of framed poem receipts is currently on display at the Open Data Institute in London as part of a commissioned exhibition on Data as Culture.

I finished my thesis, and I am now based in Edinburgh as a Post-Doc Research Associate in Creative Informatics at Edinburgh College of Art. I have just secured an Edinburgh Futures Institute research award to enable me to realise a long-standing ambition for {poem}.py. In collaboration with institutions including the National Library of Scotland, Edinburgh City of Literature, and local galleries, the funding will scope and prototype a large-scale public artwork version of {poem}.py using projections onto public spaces and buildings.

Not my intended thesis at all, but I wouldn't change a minute of it.

Dr Giovanni Cherubin – 2014 Cohort

For me the CDT programme has been much more than a PhD scholarship: it allowed me to train my personal and technical skills, it offered me the opportunity to network with industry partners and to intern with great companies, and it gave me a sense of community. Also, the CDT funding gave me enough support to attend several conferences around the world, thanks to which my research could flourish.

My journey as a CDT student begun right after I completed my MSc in Machine Learning at Royal Holloway. I had always had a passion for Information Security, which until then I had only pursued in my spare time. For the following four years, the CDT allowed me to work on this full-time, alongside my main interest, Machine Learning. The CDT gave me the great privilege to attend workshops and conferences, even when I did not have a paper to present there. This was invaluable, particularly during the first years: it helped me both to select a research topic and to find interesting problems, but also to meet PhD peers with whom I subsequently started collaborating.

One of the most important activities of my CDT years has been the 'summer project'. I selected a problem I hadn't been able to fully define at the time: can we use Machine Learning to provably measure the security of a network protocol (eg Tor) against traffic analysis attacks? I did realise the same approach could have had further applications, but I chose the problem of traffic analysis for concreteness. Before I started, I felt this project was risky: I had a rough idea of where to start, but I was not sure this problem had any solutions where I was looking; indeed, the literature until then had been very vague and rarely formal on this problem. Nevertheless, the somewhat 'risk-free' structure of the summer project with the CDT convinced me to try this, and it worked well.This work ended up being the main building block of my PhD thesis, and even now, as a postdoc researcher, I am still working on some of those ideas (by using similar principles, one can measure the security of several attacks other than traffic analysis). Had I not have been given the time and freedom to explore this idea, I might have never dedicated myself to it.

The CDT programme also put a lot of emphasis on our training. We were offered classes on presentation skills and academic writing, and also on technical skills including penetration testing, and on management and networking. We were encouraged to make academic visits and take internships, and I spent some time at Cornell Tech and then at École Polytechnique in Paris and on my industry-based internship I had a fantastic experience at HP Labs in Bristol. All in all, I feel the CDT helped all of us develop the skills required for both academic and industry careers. Right after my PhD, I went for a postdoc at EPFL in Switzerland, where I currently work at the intersection between Machine Learning and privacy.

Dr Alex Davidson – 2014 Cohort

When I think back to my time as a PhD student at Royal Holloway CDT, my overriding feeling is of being thankful for the opportunities that I was presented with. I am not just referring to being given the chance to conduct research in an Information Security department that is internationally renowned for conducting high-quality research. The PhD

programme provided me with a range of skills that helped to shape my own personal development, and the path that I will follow in the future.

My undergraduate background was in Maths, though I worked for a short time as a software developer before I started on my PhD. While I initially began with intentions of carrying out research in the area of game-theoretic modelling of cyber security situations, I altered course in my first year to studying theoretical cryptography (and secure computation). The flexibility was instrumental in me finding an appropriate research topic. Being passionate about your research makes the whole experience far more worthwhile, and so taking the time to find the right topic is essential.

As a PhD student I was given the freedom to decide which areas and research questions within the broader topic that I would like to tackle. This involved working closely with my supervisor on certain problems, and also spending time working on problems with other members of the department and fellow students. Being given this working freedom to explore difficult problems, in addition to learning from academics and peers, really is a unique experience.

My research was generally theoretical in nature, and I also undertook two internships in the Crypto team at the content delivery network Cloudflare. Cloudflare helps to reduce the latency in internet connections between clients and websites by distributing and caching resources in data centres around the world. They also implement various security natures using the strength and size of the network that they use. During my time as an intern I worked on writing a Chrome/Firefox extension called Privacy Pass that allows clients to anonymously bypass challenge mechanisms that disproportionately effect users of anonymity-preserving tools such as Tor and VPNs. This browser extension is now actively used by over 150,000 people. Working on this project was a great experience as it allowed me to apply the knowledge from my research to solve a problem with genuine societal impact.

The advantage of being a member of a well-known research department is that there are people with contacts throughout a number of different industries, and this helped in making these internships possible. My work at Cloudflare was undoubtedly more practically focused, but also resulted in research that eventually made it into my thesis. The two three-month internships helped enormously in framing the impact of the research that I was doing during my PhD.

At the end of my PhD I took a full-time role in the Crypto team at Cloudflare. The Crypto team is mostly research-oriented and attempts to engineer cryptographic solutions to problems in the security and privacy spaces. The team (and company in general) values the time taken to pursue interesting research problems, and so I have been able to keep working on solving difficult problems with real-world impact. Cloudflare serves over 10% of all requests on the internet and so the work that we do also affects the way that the internet runs on a huge scale. Working at the intersection of cryptography and globally distributed systems is not something that I ever would have imagined that I would be doing back when I started at Royal Holloway in 2014.

Finally, it is clear that I would never had these opportunities had I not participated in the CDT, and I am thankful for that. My fondest memories relate to the people that I met along the way, and the chances to learn, both personally and academically, that I was exposed to. I would encourage anyone who is currently studying to make the most of these moments to learn and progress, because it is an opportunity that does not come around too often.

The Crypto team – and Cloudflare as a whole – are always looking for new people to join as full-time employees, or as interns. If you think that this would be something that you would like to do, then please get in touch! (email:adavidson@cloudflare.com)

CDT Research newsbites

The British Computer Society and ISG awarded the David Lindsay memorial prize to first-year CDT student **Colin Putman**. The David Lindsay award is presented each academic year to the student from the Royal Holloway College who, in the opinion of the Specialist Group, submits the best MSc dissertation on an information security related topic.

Jake Massimo's work on the need for robust testing of mathematical parameters in cryptographic software led to changes being made to OpenSSL, one of the world's most widely-used cryptographic libraries (around 90% of web servers depend on it). Jake's research, carried out jointly with Steven Galbraith and Kenny Paterson, will be presented at the PKC conference in Beijing, China, in April 2019 and can be read online at **https://eprint.iacr.org/2019/032**

Torben Hansen with Kenny Paterson and Martin Albrecht had a paper accepted to the IACR Transactions on Symmetric Cryptology on implementing advanced security goals, such as defence against traffic analysis, in practice for the popular SSH protocol.

Fernando Virdia together, with Martin Albrecht, Christian Hanser (Infineon), Andrea Höller (Infineon), Thomas Pöppelmann (Infineon), and Andreas Wallner (Infineon), had a paper accepted to the IACR Transactions on Cryptographic Hardware and Embedded Systems on implementing post-quantum cryptography on a chip with an RSA co-processor, applying techniques from computer algebra to cryptography.

Pallavi Sivakumaran and Jorge Alis Blasco will be presenting their paper titled "A Study of the Feasibility of Co-located App Attacks against BLE and a Large Scale Analysis of the Current Application Layer Security Landscape" at the 28th USENIX Security Symposium 2019 this summer. The paper talks about some of the risks posed by how Android handles BLE connections and a measurement of how many apps are affected by those risks.

Eamonn Postlethwaite and his co authors Martin Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Marc Stevens, obtained several world records in solving hard lattice problems. These computational problems are poised to underpin the next generation of encryption algorithms. Their paper discussing their techniques was accepted to EUROCRYPT 2019. **https://www.latticechallenge.org/svp-challenge/index.php**

Amy Ertan has been awarded the ITS UK-Brazil Data Protection Fellowship 2019 and will be spending six weeks in Sao Paolo, Brazil, this summer. The programme enables Amy to explore global approaches to data protection and internet policies. More information can be found here: **https://itsrio.org/en/comunicados/result-uk-brazil-data-protection-fellowship-2019/**

Nick Robinson recently spent 3 months as a visiting researcher at the Ragnar Nurkse Department of Innovation and Governance at TalTech University, Tallinn, Estonia. This led to the paper, "The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis", being accepted and presented at ICEGOV'19 in Melbourne, Australia. Co-authored with Laura Kask and Prof. Robert Krimmer, this early research was nominated for best paper at the conference.

Ela Lee has recently had a paper accepted to ACISP (the 24th Australasian Conference on Information Security and Privacy) on her work on Proxy Re-Encryption with Post-Compromise Security. This paper investigates the necessary conditions for a proxy re-encryption scheme to be useful in mitigating data loss when the key used to decrypt files stored remotely is compromised.

8044 05/19

EPSRC
Engineering and Physical Sciences Research Council

www.royalholloway.ac.uk/CDT
CyberSecurityCDT@rhul.ac.uk
@RHULCyberCDT

Royal Holloway, University of London
Egham, Surrey, TW20 0EX
+44 (0)1784 434455
www.royalholloway.ac.uk