CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

Summer 2018

CDT update

Director Report: Professor Keith Martin

The EPSRC Centre for Doctoral Training in Cyber Security is now in its fifth year. I am just back from the very moving summer graduation ceremony, where the first of our CDT PhD graduates received their degrees from Principal Paul Layzell in the College Chapel. Wow – it seems like yesterday that we were designing our doctoral training programme in the beer garden of the Happy Man pub! Now we are just closing recruitment of our sixth cohort, who will commence their training in September 2018. There are plenty more PhD theses and graduation ceremonies on the way.

Special thanks

My role as Director of the CDT has been confirmed for next year, so I'd like to take this opportunity to convey my thanks to two very special people.

Professor Carlos Cid has led the CDT from its launch in 2013 until his well-earned sabbatical in 2017. Carlos has been a passionate believer in the project from the outset, designing an excellent training programme and working tirelessly to support the Centre. He has represented the CDT at countless events and given numerous talks about its work, including at the launch event in Portcullis House. He cares about every student in the CDT and knows every detail of their progress. He's also a master of the spreadsheets, knowing his way around the complexities of all the finance arrangements. Fortunately, for me, Carlos has agreed to remain involved in the ongoing CDT management. Obrigado!

As everyone who has engaged with the Centre knows, the CDT is really run by Claire Hudson. I can't thank Claire enough for her role in day-to-day support for the CDT. From managing admissions, dealing with student inquiries, running our events, liaising with the College, to acting as the first point of contact for the CDT, Claire is doing a magnificent job. From a CDT student perspective, while the academics are the annoying people behind the scenes who make unreasonable demands on their time, Claire is the friend who makes things happen. Many thanks to Claire, from staff and students alike.

Every PhD is special

You will read elsewhere in this newsletter about yet more incredible success stories from the CDT, including awards, high-profile publications and research having real impact, and it is right to promote and celebrate these achievements. However, it is also easy to forget that every PhD journey is special in its own way, and not all students are stacking prizes on their mantelpiece. A PhD is an apprenticeship in the conducting of research, and every student who completes the degree is receiving recognition for mastering skills such as the ability to analyse the work of others and to communicate new ideas. Students within the CDT are also equipped with an excellent range of transferable skills, as well as experiencing a range of interactions with the wider cyber security profession including, in almost all cases, an internship. Every PhD is its own success story.

New CDT proposal

Is 2018 our last cohort of CDT students? We sincerely hope not, and are delighted to report that our funding bid to continue the work of the CDT has progressed to the next evaluation phase. In our new proposal, we have extended the scope of our existing CDT and revamped the training programme in order to have a broader focus on the social, as well as technical, aspects of cyber security. We will learn whether this bid has been successful towards the end of this year.

Inside the cohort

Jeroen Pijnenburg – 2017 Cohort

Our cohort is fast approaching the end of the first year. While the heat rises and Egham's population diminishes, we are all hard at work on our summer projects. Everyone is now on their own schedule and working in different locations. The first year has been a great experience preparing us for this. Of course we have done a lot of courses, seminars, workshops, company visits and discussions – from agency to algorithms – which has been very practical and useful. We have developed our own skill set and we have seen cyber security from many different perspectives and yet come to realise it all intertwines.

However, we did all of these activities together. It connected us and it bonded us. Over the past year our cohort has been carefully forged by a seemingly invisible hand into what it is today: a connected network of highly specialist individual nodes. We still have our own identity and expertise, but we have learnt how to communicate across different disciplines and how to work together.

So even though we are now rarely at the same place at the same time, these relations have been formed and we know how to find each other when we need help, advice or a laugh. I am positive they will be maintained for many years to come. We have created an invaluable resource we can exploit for the benefit of our PhDs, and our lives in general.

Eamonn Postlethwaite – 2016 Cohort

For me, the ease of transition between the taught component of the CDT programme and the much longer, more traditional, research component can mostly be attributed to the encouraging academic atmosphere and excellent supervision offered by the department. As undergraduate and masters degrees in the UK arguably become more about learning for examination, the culture shock a PhD student can feel when faced with the slow, deliberate and thoughtful work required to understand a topic sufficiently well enough to contribute can be intimidating. For example, here is a list of things that seem outwardly obvious but took quite a lot of time to internalise: I am not expected to know everything; it is fine to spend a few months learning a new area; it is fine to submit your first piece of serious work more than a year in; and many more. In short, as long as you can look yourself in the mirror and know that you are putting the work in on a regular basis, you are almost certainly doing fine. Embracing the above facts can also lead to a pleasantly "gung-ho" attitude of asking anyone anything at any time.

So, what in the department convinced me of the above truths? Not being expected to know everything is easy: simply go along to a seminar/coffee break/dinner and observe a titan in their respective field ask an entry-level question about a different field without a shadow of embarrassment. To see a few months is reasonable to dip your toes into a new area, consider the summer project. I studied a class of algorithms known as lattice sieves, which find short vectors in high dimensional lattices, and it took me three solid months of reading to come away with an entry level understanding of the field. Looking back, I cannot see how I could have been much more efficient about it. Not worrying about when your first paper will come out is mostly down to your supervisor. If they are happy with the progress of things, then you probably should be too. This touches on another important element of this transition from taught to research, which is the excellent academic and pastoral care I have received from my supervisory team. From the initial nudges in the direction of great (interesting and active) research topics, to the perfect balance of leaving me to be stuck and creative on my own vs. useful advice which facilitates progress, I could not have asked for more. Trust me, it is shockingly easy to go from worrying about not having enough potential projects to worrying about having too many.

Two years in to the CDT, I am enjoying myself more than ever, and feel as if my abilities and confidence as a researcher have grown enormously. The moral of the tale? Don't panic!

CDT Showcase Event

On Wednesday 9th May, we were joined by industry and academic colleagues for our annual showcase event, this year held at Cumberland Lodge in Windsor Great Park.

Our showcase event, now in its fifth year, provides us the opportunity to demonstrate the strength and diversity of cyber security research being conducted by our students, and this year, along with a variety of short talks from students, we enjoyed a poster session, a 'Dragons Den' session for first year students and an interactive session around the subject of 'Skills for Cyber Leadership'.

Posters on show illustrated the CDTs research in a variety of areas including Privacy, Security and Trust in healthcare, Authentication Permissions using Bluetooth and Maritime Cyber Security. The students were on hand to present their posters and further explain their research to our guests. Our interactive session was an informal but lively event in which we were hoping to exploit the knowledge of our room full of experts and draw on their understanding surrounding the issue of the skills required for Cyber Leadership. The feedback from this short session was fruitful and we will be looking to introduce some of the findings into our CDT programme for the coming years. The day concluded with a presentation from Dr Thyla van der Merwe, one of the CDT students in our first cohort. Thyla, who later graduated in our July ceremony, thanked the CDT for enabling her to develop her career and added that the CDT provided many opportunities to connect with industry experts and academics and fellow students specialising in this field.

One of our invited guests, James Cawley, CTO – Cyber Security, L3 TRL commented *"Please allow me to express my thanks for the experience of attending the CDT showcase event at Cumberland Lodge on May the 9th. It was a well-run event in a beautiful location and a good chance to experience the diversity of research that is occurring at the University. As someone who graduated two decades ago now, even meeting postgraduate students has the potential to make one feel old, however at the same time, when I joined a group in order to discuss opportunities to evolve the syllabus, I was impressed by the maturity of the students. In particular, the way they expressed their ideas, opinions, experiences, and finally how they interacted and behaved as a team. This I am sure is partly thanks to events like this in terms of encouraging presentation skills, interactions with peers and external guests and finally will make any Royal Holloway CDT graduate an asset to future employers".*

Our next Showcase event is scheduled for 8 May 2019, again at Cumberland Lodge.
We hope to see you there!

CDT research newsbites

The Andreas Pfitzmann best student paper: "Privacy Pass: By passing Internet Challenges Anonymously" was awarded to CDT student **Alex Davidson** and co-Authors (Ian Goldberg, Nick Sullivan, George Tankersley, Filippo Valsorda) at PETS 18

Pip Thornton is leading the way with her innovative research investigating poetry and Google AdWords. Her article on Google and language 'A Critique of Linguistic Capitalism: Provocation/Intervention' is published online in GeoHumanties **tandfonline.com/doi/full/10.1080/2373566X.2018.1486724**

Pip Thornton also won the Best Poster Award at the 10th International ACM Conference on Web Science for her poster, also titled 'A Critique of Linguistic Capitalism'.

Feargus Pendlebury co-authored a paper on an analysis of and case for robust evaluation of machine learning classifiers in security research.

Why are 50,000 ships so vulnerable to cyberattacks? **Professor Keith Martin** and CDT student **Rory Hopcraft**, explain the reasons in The Conversation UK. Read their article at **socsi.in/2Tv3z**

Giovanni Cherubin wrote an FAQ-style blog post, generalising his work on security bounds for WF defences to the problem of estimating the security of generic black-boxes. View this at **giocher.com/pages/bayes.html**

New Statesman published a piece by **Andreas Haggman** in which he explains the strategy behind his tabletop wargame based on the UK National Cyber Security Strategy **newstatesman.com/spotlight/cyber/2018/05/why-policymakers-are-playing-board-games-counter-cyber-threats**

The best paper award at the Conference on Cryptographic Hardware and Embedded Systems (CHES 2018) was to **Amit Deo** and his supervisors **Professor Kenny Paterson** and **Dr Martin Albrecht** for their paper 'Cold Boot Attacks on Ring and Module LWE Keys under the NTT'.

During his internship at CloudFlare, **Blake Loring** implemented a solution to the BREACH compression side-channel attack against TLS that can be deployed at scale. He explains the technical aspects and presents a challenge site in a blog post at **blog.cloudflare.com/a-solution-to-compression-oracles-on-the-web/**

Angela Heeler was the only UK student to give a talk at the Academic Centres of Excellence in Cyber Security Research (ACE-CSR) conference. Her presentation, titled "Securing London's SMEs" was well received and resulted in some exciting opportunities to meet with senior personnel from academia and government.

CDT team win Cyber 9/12 competition

In February 2018, a team from the CDT took part in the first Cyber 9/12 competition based in the UK, competing over three rounds and eventually winning the competition. The multi-disciplinary team, with backgrounds in small-medium business and IT management, cryptography, Philosophy, Politics, Economics (PPE) and Psychology was made up of year-one students Amy Ertan, Angela Heeler and Georgia Crossland along with year-three student Lydia Garms.

For the first round, several weeks before the event, the team were provided with an intelligence pack consisting of a collection of sources on a potential threat to the UK, involving a vulnerability to UK airports, manipulation of aviation financial markets, a new internet of things botnet, and a social media botnet. The team were tasked with preparing a 500-word brief summarising the scenario and a decision document to outline three potential policies in responses to this situation including a preferred option.

On the first day, the team gave a ten-minute presentation on their policies, followed by a short Q&A with the judges. Their performance in this round saw them through to the semi-finals where they were provided with another intelligence pack, in which the situation had escalated, and cyber-attacks had caused disruption to several UK airports and the UK banking system. Working through the night, the team produced another decision document detailing a new set of policies. Their finished document was presented the following morning, where it was later announced

Robert Carolina (Coach), Georgia Crossland, Amy Ertan, Lydia Garms, Angela Heeler

that they were one of four teams to make it to the final round. In this session, they heard how the situation had escalated even further, with a potential attack on UK airspace that could lead to loss of life, and could be attributed to the fictional country of Mordonia. With just 20 minutes to read a new intelligence pack, decide on three new policies, and prepare for the presentation, (all whilst in isolation with no access to laptops or other devices,) the team were eventually delighted to discover that they had won the competition, concluding an amazing end to a high pressured but enjoyable two days.The competition highlighted the effectiveness of multi-disciplinary approaches to cyber security. Within the team, each member effectively handled an area in which they had direct experience, but as individuals, each felt they had been challenged through the competition whilst learning from other disciplines.

"I am immensely proud of Team CDT. Their victory in this year's London Cyber 9/12 Competition was a testament to their dedication and teamwork. Their achievement should send a signal to the entire cyber security community about the power of using interdisciplinary teams to attack cyber security problems. I'm grateful that their achievement has been recognised with this prestigious award." Robert Carolina, team coach.

Team CDT commented 'Competing in the 9/12 cyber policy competition was an incredible experience, and it was amazing to be subsequently nominated for Cyber Security Student of the Year award. We all had a wonderful time at the awards ceremony – and it was the ultimate surprise to be awarded as winners! Overall it's been a great learning experience and our pleasure to represent the university, meeting other talented students, researchers and industry professionals.'

All female team win Cyber Security Students of the Year, 2018

The same team who won the Cyber 9/12 competition continued their victorious journey by scooping another prestigious prize with leading cyber security publication, SC Magazine.

The all-female team, picked up the award for Cyber Security Students of the Year at the 2018 SC Europe Awards ceremony in London on 5 June 2018. The Cyber Security Students of the Year award celebrates current students pursuing degrees in cyber-security and cyber-security related fields.

Angela Heeler, Lydia Garms, Georgia Crossland, Amy Ertan

SC 2018 awards EUROPE

The growing demand for cyber-security professionals has led both government and industry to introduce initiatives to increase the range and variety of cyber-security relevant courses, supplemented by competitions that also draw in mature students and nonSTEM candidates. Now there are GCHQ accredited cyber-related Masters, competitions for schools, universities, and open access. There are brilliant individual students conducting both theoretical and practical research, up to and including the launch of new products and services, and there are teams of students banding together to take on the challenge of simulations.

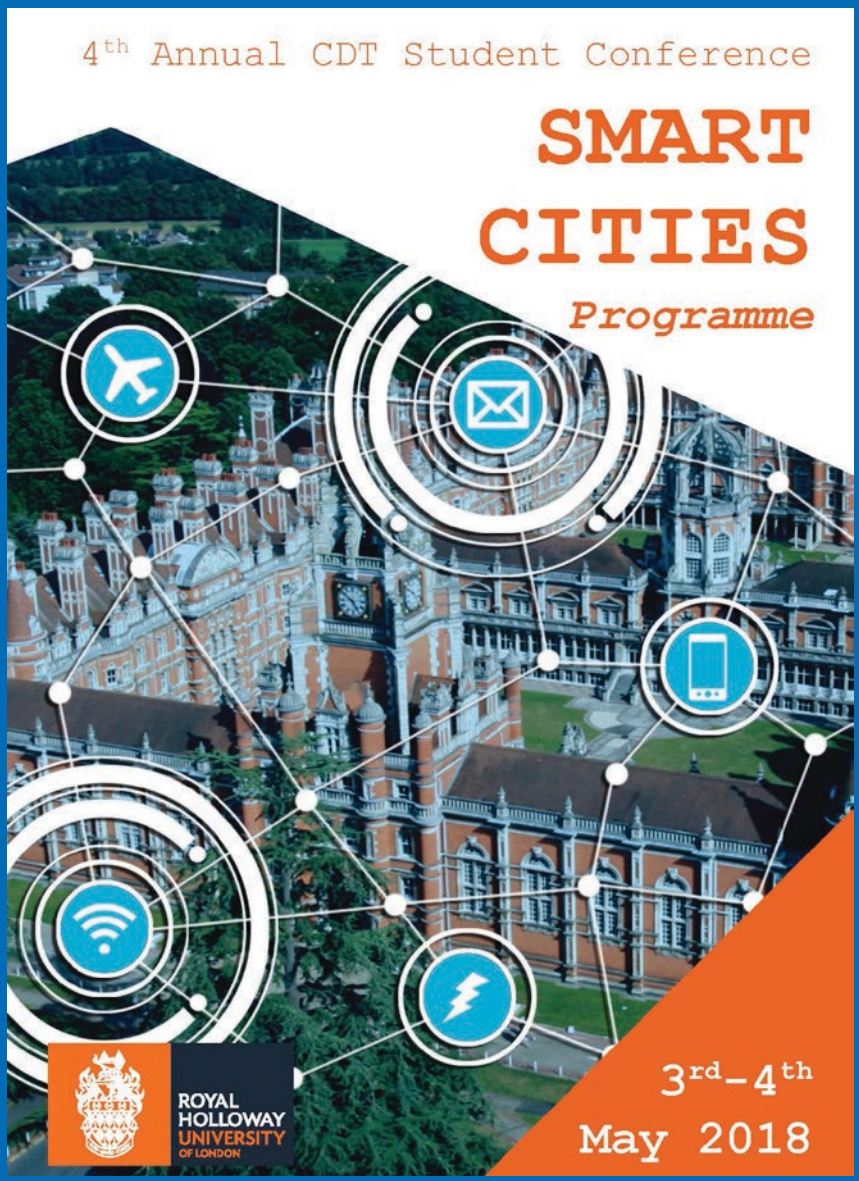
This year's winners , Team CDT, was formed based on diverse backgrounds of small-business, technical, economics/ politics and psychology, comprising Georgia Crossland, Amy Ertan, Lydia Garms and Angela Heeler, students at Royal Holloway, University of London, who were also winners of the Atlantic Council UK Cyber 9/12 Policy Competition 2018. This competition entailed demonstrating, within a competitive environment, not just ability to identify, comprehend and manage appropriate response to a simulated cyber-attack, but also to be able to effectively communicate what was happening to nonspecialist government decision makers - the Prime-Minister's advisors. Thus, they needed to show both technical and operational skills as well as strategic risk analysis, turning data into actionable intelligence at both the operational and strategic level. Truly a test of the skills we need in our CISOs of the future.

www.scawardseurope.com

Royal Holloway host the inter-CDT conference on 'Smart Cities'

Early May saw the arrival of the 4th annual inter-CDT workshop, this year hosted by Royal Holloway. The theme was 'Smart Cities' and what followed was a rich and interdisciplinary discussion of what a smart city was and what it could look like.

Day 1 began with the Head of Oxford CDT programme, Andrew Martin, highlighting some of the key themes and questions smart cities raise. He was followed by Joe Dauncey of Inmarsat, who described the organisation's various smart city projects, particularly relating to efforts to develop 'smarter', more efficient control systems. Paolo Cardullo from Maynooth University then led a discussion on the implications of the smart city on citizenship, exploring what a smart citizen might look like. From the University of Neuchâtel, Sarah Widmer discussed her research on the location-based social media app, Foursquare, in order to think about how data-driven cities are practically lived in today. The issue of privacy was highlighted by Panos Papadimitratos from the KHT Royal Institute of Technology, discussing security related issues in urban sensing systems, and giving examples of how the smart city could be technically implemented and what issues this raises. The day was drawn to a close by a student-led debate. Chaired by Andreas Haggman, the question was:



'Do the benefits of smart cities outweigh the drawbacks for cyber security?' The 'For' side was argued by RHUL's Jordy Gennissen and Oxford's Marcel Stolz, with the 'Against' argument headed by Ela Berners-Lee from RHUL and Sean Sirur from Oxford. Through a heated and varied discussion, particularly relating to the political implications of a 'truly' smart city, both debaters and audience found it challenging to decide firmly on one side of the debate, marking an official draw between the teams. The conversations continued over dinner and drinks.

Day 2 was kicked off by Matthew Cook from the Open University who explained how the smart city narrative had been demonstrated in practice when constructing Milton Keynes. Jarmo Eskelinen presented the work of the Future Cities Catapult, highlighting the positive and negative opportunities that smart cities provide. From the Oxford Internet Institute, Jonathan Bright presented a whistle-stop tour of the ways in which the smart city is already upon us, based on his interests in data science and electronic government. Andy Jones then reflected on the question of 'How do we survive the 'Cyber City?', and related to his varied cyber security career experiences, most notably as CISO of Maersk when they were heavily impacted by the NotPetya attack. The final conference presentation was from Oxford CDT student Andrew Dwyer, who talked about mappings and representations of the cyberspace and the smart city.

Professor Keith Martin concluded the event by discussing the smart city as a thinking tool or proxy for the future. Although it is difficult to come to confident conclusions in an area with vast unknowns and uncertainties about the future, the workshop encouraged students to think critically about the smart city and what it can offer.

A full blogpost on the event can be viewed here **rhulgeopolitics.wordpress.com/2018/06/08/smart-cities-rhul-hosts-inter-cdt-workshop/**

Royal Holloway look forward to passing on the baton to Oxford for 2019. Follow tweets from the workshop at #CDTSmartCities to stay updated.

Away from the Ivory Tower

Reflection on Internships

Torben Hansen – 2015 Cohort

This Spring I was fortunate to have the opportunity to intern at Amazon Web Services (AWS) in Seattle. Simply put, AWS provides Infrastructure-as-a-service together with a plethora of web services (cryptography related services entail KMS, ACM and CloudHSM). These services help companies reduce the complexity of providing, e.g. availability, redundancy, security and scalability of IT. AWS works at an unbelievable scale, and service many well-known companies: Netflix, Spotify, Airbnb, General Electric, Siemens, Slack, and the list goes on and on. AWS is truly scale of scale.

Part of my work as an intern was to specify hybrid key exchange methods in SSH and prototype these in an SSH implementation. The work was done in relation to the ongoing post-quantum cryptography "competition" run by the US National Institute of Standards and Technology (NIST), where AWS has contributed to two submissions: BIKE and SIKE.

SSH is a widely used and supported secure communication. Unfortunately, the current cryptographic algorithms used in SSH are insecure against quantum adversaries, i.e. bad people that have access to a large quantum computer. A hybrid key exchange method is an attempt to thwart attacks by such adversaries, by combining a current cryptographic algorithm with a new post-quantum cryptographic algorithm. But since post-quantum algorithms are new, they do not yet possess a high level of trust. However, the hybrid key exchange method construction remains secure even if a post-quantum cryptographic algorithm turns out not to be cryptographically secure. The hybrid key exchange method prototypes and specification have both been contributed by AWS to the Open Quantum Safe project.

Being an intern at AWS was a fantastic experience. Interns are treated as regular employees, given responsibility, and have the chance to contribute code to production systems used by millions and millions of people. Also, a nice perk of interning at AWS in Seattle is that dogs are allowed in AWS offices. So, if some problem is frustrating you, canine help is always near!

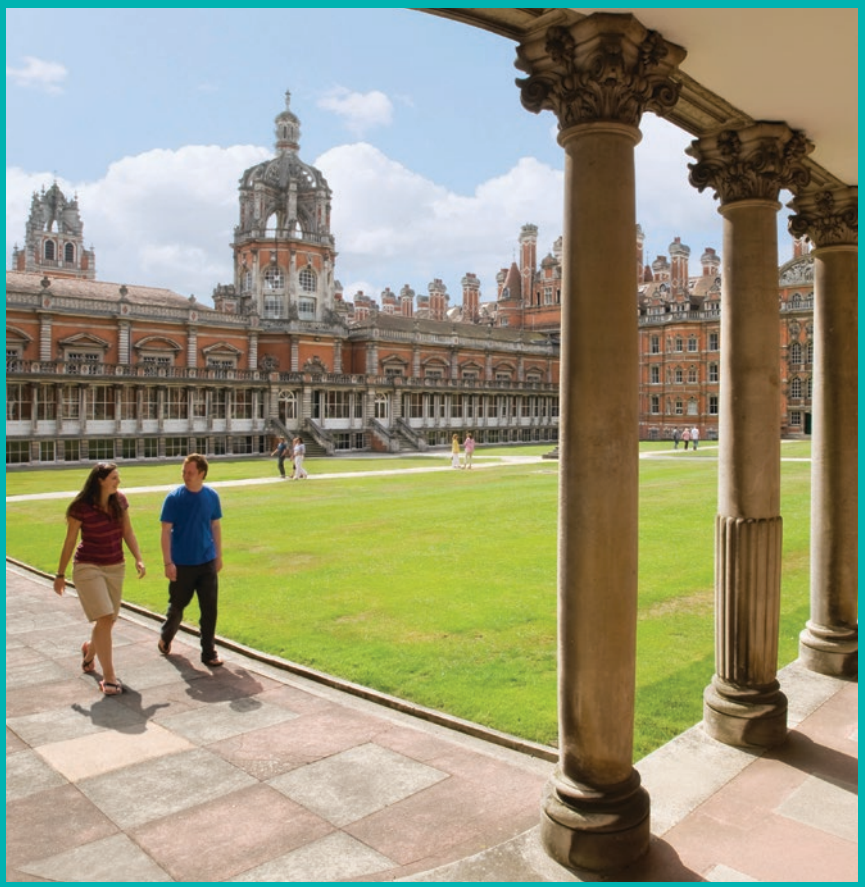
Ela Berners-Lee – 2014 Cohort.

As part of my CDT training, I undertook a six-month internship at Crypto Quantique - a startup based in London. Crypto Quantique have developed a microchip where each chip generates unique randomness. Since good randomness are needed for keys, which are the foundation of secure cryptography, this is very exciting.

In my PhD much of my work has been more on the theoretical side, so it was good for me to gain an appreciation for implementation and the challenges it presents. For example, I spent some time considering alternatives for post-processing that are more power-friendly, so the product would be more suitable for IoT environments where battery power is precious.

I was very fortunate in that my experience wasn't limited to the technical. I also gained an appreciation for the business case, getting to sit in on meetings with potential partners and contribute to the discussion. I also had a good degree of freedom in my work. Whilst I had some set tasks, I was given the freedom to explore ways in which the chip could be used to create novel crypto solutions. It was a great exercise in being able to explain my ideas, why I thought these would work well for the chip, and why this would present a unique solution that would be of interest to clients.

Overall I am very grateful to Crypto Quantique for the experience, and thankful for the CDT model for encouraging us to spend time outside academia to see how useful our expertise is in the real world.



CDT News

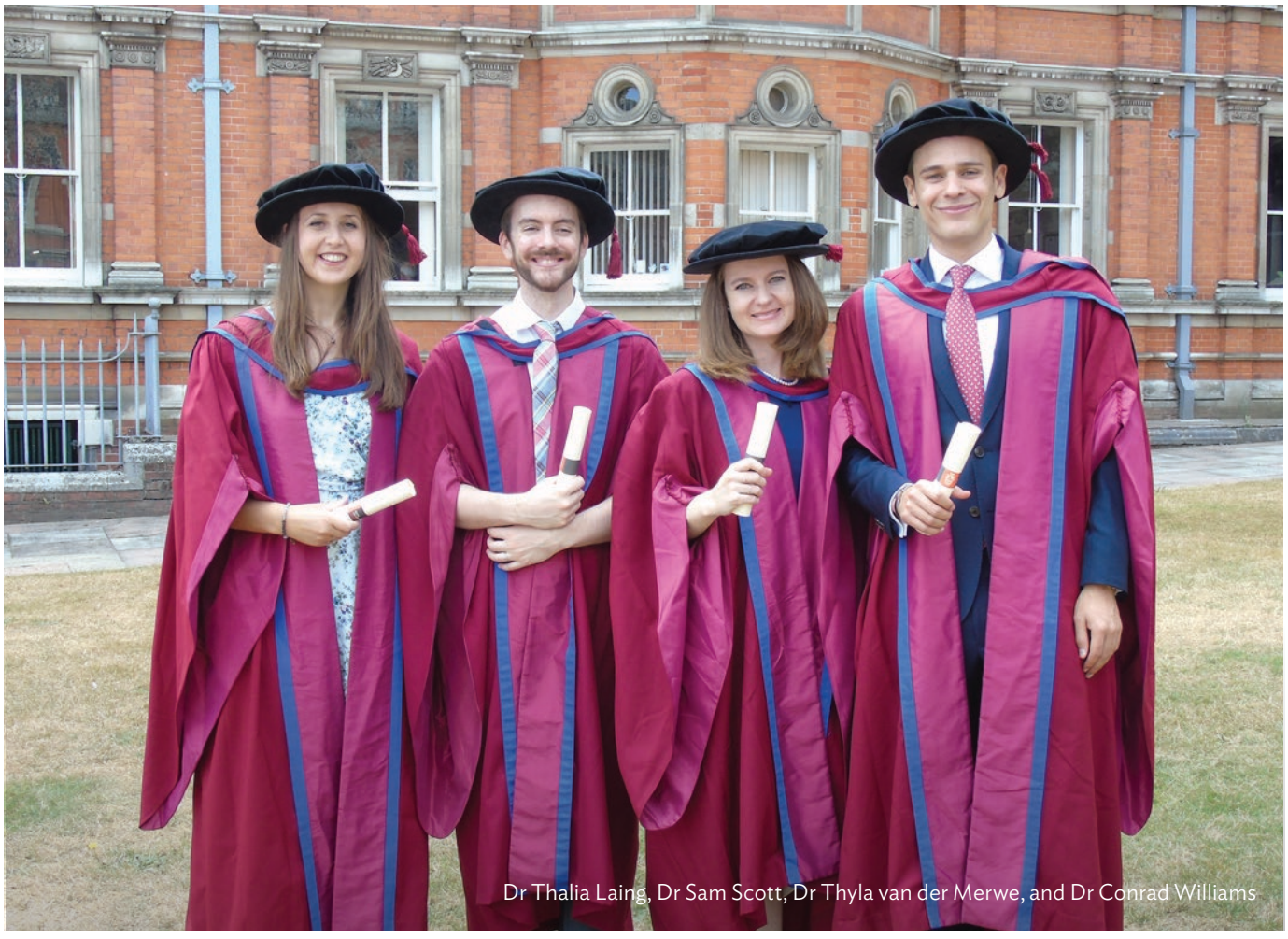
Graduation

In July, we celebrated alongside the first graduates from the CDT in Cyber Security. This was a special experience, allowing ISG academics to celebrate alongside our first graduating students whilst enjoying the stunning surroundings of our famous Founder's Building.

Dr Sam Scott reflected on his CDT experience:

"The CDT helped me in many ways. Throughout my time as a student, I had the opportunity to discover the areas of research which most interested me, spent time meeting with people from diverse fields and explored the many aspects of cybersecurity. In my opinion this approach is invaluable to anyone, whether considering an academic career, or one in industry. A wider understanding of the field makes you a better researcher, but also helps you to appreciate the value of the deeper knowledge you acquire in your specific area. As I start a new adventure building a cybersecurity startup, I am incredibly grateful to have had the opportunity to be one of the early CDT members, for everything I learnt, and all of the people I encountered."

Sam is now on the Runway Startup Postdoc program at Cornell Tech in New York, a program designed for people in technical fields finishing PhD studies, who want to commercialise their research and ultimately build a business around it. Sam is the founder and CEO of kee.sh, a cloud-native secrets management service, helping companies to automate and integrate secrets into their development pipelines. kee.sh takes a developer-centric focus on secrets, and provides the tools necessary to provide, distribute, and audit secrets, without the need for running additional infrastructure. We wish Dr Thalia Laing, Dr Sam Scott, Dr Thyla van der Merwe, and Dr Conrad Williams every success in the future.



Dr Thalia Laing, Dr Sam Scott, Dr Thyla van der Merwe, and Dr Conrad Williams

7913 08/17

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