# Information Security Group

Review 19/20

ROYAL HOLLOWAY UNIVERSITY OF LONDON

# WELCOME — LIVING WITH CHANGE PART 2

Peter Komisarczuk

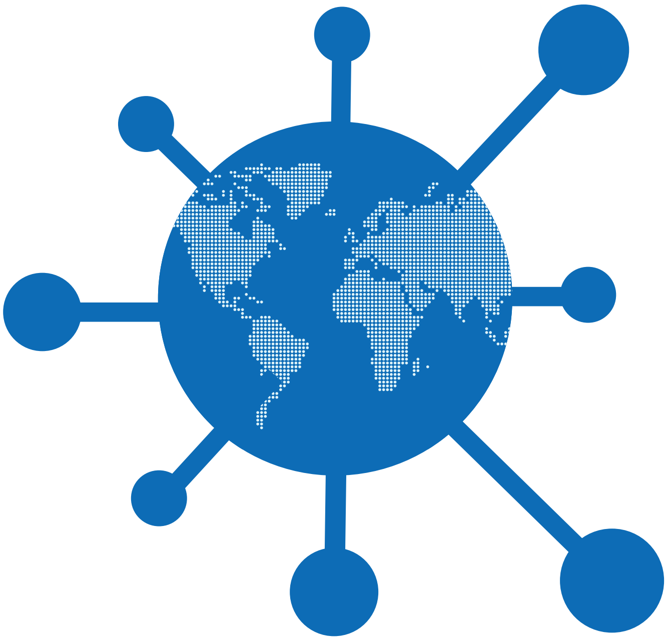
> Professor ISG, Director, Information Security Group

Welcome to the 2019-20 ISG review, our 30th year. Last year I entitled the introduction as "living with change" and I continue in that theme again. This year's review finds the ISG in interesting times as we worked through the changes started in 2018-19 and now also the changes brought about because of the COVID-19 pandemic. My introduction provides a brief overview of some of the developments this past year and it gives me an opportunity to thank colleagues and students as they deal with the changes we have faced and the new challenges for the next academic year.

There are many aspects around this review that remain similar to last year – good student numbers at both undergraduate and postgraduate levels, more successes in research funding, excellent research outputs and impactful work with industry, standardisation and government. We have seen success with £5m from the EM3 LEP to fund a cyber security and big data institute which is to be housed in a new innovation building on campus, as well as new forays into the cyber innovation space. In 2019-20 the ISG has seen three CyberASAP funded start-ups developed by members of the ISG. These are in various areas of cyber security led by Jorge Blasco Alis, Kostas Markantonakis and Raja Akram. The work on these start-ups has continued throughout the year with two continuing under CyberASAP phase 2 funding and one continuing through an ICURe innovation to commercialisation grant. Throughout this review, colleagues and students discuss their many and varied research, outreach and other activities over this past year.

In the autumn we welcomed three new colleagues as lecturers to the ISG. Jassim Happa joined us from Oxford, Darren Hurley-Smith from Kent and Rachel Player from a postdoc position in the ISG. They have all hit the ground running and have taken on leadership of modules, student supervisions and applied for research funding. We introduce them in this review and wish them a long, happy and rewarding time in the ISG. We were hoping to further add to our numbers and in January 2020 advertised for two more lecturers to join the ISG. Unfortunately, due to the current situation, these two positions have been put on hold for now.

We celebrated two significant milestones this past year. Firstly, 2020 is the 30th year of the ISG. We reflect on these 30 years later in this review through the thoughts of some of its founding members. Secondly, and more significantly, at the 2019 HP Colloquium we marked the official (re-)retirement of Fred Piper. We reprint the words of Rob Carolina's short tribute to Fred at the Colloquium and I echo our thanks to Fred for who he is and all that he has done.



INDEX

03 MSC UPDATE
04 WHAT IS INFORMATION SECURITY?
05 A NEW POPULAR SCIENCE BOOK ABOUT CRYPTOGRAPHY
06 WELCOME
08 THE IMPACT OF QUANTUM COMPUTING ON MOBILE SECURITY
09 BEHAVIOUR CHANGE: CHALLENGES FOR INFORMATION SECURITY
10 DOING WHAT YOU CAN IN A TIME OF CRISIS
11 THIRTY YEARS* OF THE INFORMATION SECURITY GROUP
14 WRITING FOR PUBLICATION: AN OPPORTUNITY FOR GRADUATE AND POSTGRADUATE STUDENTS
15 CRYPTOGRAPHIC SECURITY PROOFS AS DYNAMIC MALWARE ANALYSIS
16 THREE WEEKS IN CALAIS
18 WISDOM 2019-2020 ROUND-UP
19 ON THE OCCASION OF PROFESSOR FRED PIPER'S RE-RETIREMENT
20 HOMOMORPHIC ENCRYPTION STANDARDISATION
21 RESOURCE ESTIMATION GONE QUANTUM
22 UPDATES ON THE SYSTEMS & SOFTWARE SECURITY LAB (S3LAB) - 2020
24 ALL ROADS LEAD TO PEOPLE…
26 ALGORITHM SUBSTITUTION ATTACKS AGAINST RECEIVERS
27 ERROR-CORRECTING CODES: CRYPTOGRAPHY AND TELECOMMUNICATION
28 CONTACT

# MSC UPDATE

Jorge Blasco Alis

> Senior Lecturer ISG,
MSc programme director

The ISG launched the MSc in Information Security in 1992. The MSc was the first of its kind anywhere in the world. From its inception the MSc has always been aimed at meeting the needs of the real world, and the ISG has continued to maintain and develop its strong links with industry and government, whilst reaching out to wider local, national and international communities.

Since our first cohort of 10 students, our student population has not only grown, it has also become increasingly diverse. In the last five years, we have received students from more than 60 different countries with an average of 27 different nationalities per cohort. Half of our student population is 25 years old and over, with many of those being professionals working in industry who want to upskill and receive a well-recognised degree with NCSC certification. Our efforts in attracting more women to the degree are also working. In 2016 our female student population was 19%. In 2019 we reached an all-time high with 29% of our students being women. We wouldn't have been able to achieve this without the support of the Women In the Security Domain and/Or Mathematics (WISDOM) group, which is also open to our MSc students. This means that they can benefit from a range of events and activities organised by the WISDOM group, during their time at Royal Holloway.

When we started the academic year, we thought that we would be focusing on the improvements and updates we implement every year to keep our MSc at the forefront of information security. We were wrong. By the end of March 2020 more than 100 countries (including the UK) instituted full or partial lockdowns as an effort to contain the spread of COVID-19. The global pandemic is affecting every society, every community and every individual in ways we could not have imagined. From an academic point of view, this has meant the end of face-to-face teaching. In a single day, ISG academics transitioned to online teaching. This was met with an incredible response from our students, who kept participating and engaging in every lecture. As the Programme Director, I am very proud of all my colleagues and students; how they have kept the MSc community together in these difficult and challenging times.

In the past, our MSc has been known for its flexible teaching delivery options, including distance learning and block mode delivery. Now, we are actively preparing to become even more flexible in how we deliver our MSc next academic year. This will help us and our students adapt to the quickly changing circumstances we face in the coming months.

I would like to finish this yearly update on a positive note. Each year, the British Computing Society awards the David Lindsay memorial prize to one of our MSc students. This award is presented to the student who, in the opinion of a selection panel, submits the best dissertation on an information security related topic. This year, the prize was awarded to Keno Schwalb for a dissertation on ".NET" malware. Congratulations!!

# WHAT IS INFORMATION SECURITY?

Martin R. Albrecht
Rikke Bjerg Jensen

> Professor ISG
> Senior Lecturer ISG

The most fundamental task in information security is to establish what we mean by (information) security.

A possible answer to this question is given in countless LinkedIn posts, thought-leader blog entries and industry white papers: Confidentiality, Integrity, Availability. Since the vacuity of the "CIA Triad" is covered in the first lecture of the Security Management module of our MSc, we will assume our readers are familiar with it and will avoid this non-starter. Let us consider the matter more closely.

One subfield of information security that takes great care in tending to its definitions is cryptography. For example, Katz and Lindell [6, p.XV] write: "A key intellectual contribution of modern cryptography has been the recognition that formal definitions of security are an essential first step in the design of any cryptographic primitive or protocol". Indeed, finding the correct security definition for a cryptographic primitive or protocol is a critical part of cryptographic work. That these definitions can be non-intuitive yet correct is made acutely apparent when asking students in class to come up with ideas of what it could mean for a block cipher to be secure. They never arrive at PRP security but propose security notions that are, well, broken.

Fine, we can grant cryptography that it knows how to define what a secure block cipher is. That is, we can know what is meant by it being secure, but does that imply that *we* are? Cryptographic security notions – and everything that depends on them – do not exist in a vacuum, they have reasons to be. While the immediate objects of cryptography are not social relations, it presumes and models them. This fact is readily acknowledged in the introductions of cryptographic papers where authors illustrate the utility of their proposed constructions by reference to some social situation where several parties have conflicting ends but a need or desire to interact. Yet, this part of the definitional work has not received the same rigour from the cryptographic community as complexity theoretic and mathematical questions. For example, Goldreich [6, p.XV] writes: "The foundations of cryptography are the paradigms, approaches, and techniques used to conceptualize, define, and provide solutions to natural 'security concerns' ". Following Blanchette [1, p.89] we may ask back: "How does one identify such 'natural security concerns'? On these questions, the literature remains silent."

The broader social sciences offer a wealth of approaches to answering questions about social situations, relations, (collective) needs, imaginations and desires, yet, they are often relegated to a service role in information security, e.g. to perform usability testing of existing security technologies or as a token to blame the failings of such technologies on those who rely on them (see the "social engineering" literature). In contrast, we argue for a rather different intersection of social and computer science; one where social science establishes what technology is and ought to be.
The service relation is all but inverted. If anything, computer science is asked to provide solutions to problems and challenges that social science identifies. To establish what security means within social settings – to identify and understand "natural security concerns" – one approach stands out in promising deep and detailed insights: ethnography.

More specifically, as highlighted by [5, p.550], ethnography is uniquely placed to "unearth what the group (under study) takes for granted". A key challenge in engaging those who depend on security technology is that they are not trained information security professionals. They do not know and, indeed, should not need to know that confidentiality requires integrity, that existing onboarding practices can be phrased in the language of information security, which different security notions cannot be achieved simultaneously and what guarantees, say, cryptography, can give if asked. Therefore, to know exactly what is taken for granted, or put otherwise, expected, in social interactions, social and technical protocols and, indeed, cryptography, rather than what has been proven in some Appendix, is of critical import.

Some often used social science methods, while much more practical and less time consuming than ethnography, are therefore less suitable research approaches in this context. For example, questionnaires and surveys, both the qualitative and quantitative kind, are fairly futile means of enquiry here. While interviews provide some opportunity for deeper engagement, ethnography allows us to learn that which people do not know themselves. Through close observations and analysis of everyday activities and relations, ethnography reveals "the knowledge and meaning structures that provide the blueprint for social action" [5, p.551] within the group under study. The exploratory nature of ethnographic enquiry, rooted in fieldwork with the group it aims to understand, is thus a key enabler in unlocking an understanding of individual and collective security needs and practices (i.e. "natural security concerns"). The inherently reflexive and embedded nature of ethnography enables such insights.

Researchers in the ISG are pursuing this approach; bringing cryptography and ethnography into conversation. We are currently engaged in a research project concerning questions about the role security technologies, especially cryptography, can play for participants in large-scale, urban protests. How do we conceptualise confidentiality in chat groups of 50K participants, where at least some must be assumed to be infiltrators? Do notions of post-compromise security, which is a common design goal in cryptographic messaging, matter?  Does Blanchette's critique of non-repudiation as a cryptographic design goal have teeth here? What are the implicit security protocols followed by participants in these protests? Should we reorient the role of trusted-third parties in cryptographic protocols from Goldreich's "pivotal question" – "the extent to which [an] (imaginary) trusted party can be 'emulated' by the mutually distrustful parties" [4, p.600] to one where the parties are insecure but their infrastructure is not [2]? Armed with this knowledge we can then investigate whether the technologies the participants of such protests and resistance movements use provide the quality which we call "security".

References

[1] Jean-François Blanchette. Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents. MIT Press, 2012.

[2] Ksenia Ermoshina, Harry Halpin, and Francesca Musiani. Can Johnny build a protocol? co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols. In European Workshop on Usable Security, 2017.

[3] Oded Goldreich. Foundations of Cryptography: Volume 1, Basic Tools. Cambridge University Press, 2004.

[4] Oded Goldreich. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, 2009.

[5] Steve Herbert. For ethnography. Progress in human geography, 24(4):550–568, 2000.

[6] Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography. Chapman and Hall/CRC, 2014.

# A NEW POPULAR SCIENCE BOOK ABOUT CRYPTOGRAPHY

Keith Martin

> Professor ISG

I have just written another book about cryptography. Why? It's a good question! Maybe because I enjoy writing. Maybe because I felt I had something to say. Maybe, also, because I think cryptography matters to everyone, but not everyone realises.

My first book, Everyday Cryptography, is, at heart, a textbook. I decided to write it because I encountered a steady stream of requests from students on the Introduction to Cryptography module of Royal Holloway's MSc Information Security asking for recommended background reading, and I struggled to suggest any. This module adopts a non-mathematical approach to cryptography but most books tackle this subject as an application of mathematics, so were not suitable. Fred Piper and Sean Murphy wrote an excellent Very Short Introduction to Cryptography, but it is exactly what it claims to be on the cover: very short! It's a useful early read, but does not provide enough detail to support students on a postgraduate programme. Everyday Cryptography provides this missing resource. Writing such a book is a huge task and by the time I had prepared the second edition of Everyday Cryptography, I felt I was done with book writing…

Wrong! The motivation to start the whole process all over again came from three very different places.

While Everyday Cryptography is primarily a textbook and guide for security professionals trying to get to grips with cryptography, I also entertained a vague hope that a (keen) general interest reader might be able to engage with it. I soon realised this was a fantasy, particularly after my father (who has a mathematical background) confessed to having started to read it, but eventually found it too heavy going. A more general reader would clearly need a different kind of book.

In December 2015, I attended a talk by the BBC's security correspondent Gordon Corera, author of the superb book Intercept, which discusses the history of surveillance. Although he clearly had a deep appreciation of the importance of cryptography, I was struck by his deference and hesitation whenever he strayed close to discussing cryptographic technology itself. This reaction is one I have seen repeatedly among professionals working in cybersecurity. It made me think: if these guys are uncomfortable with their own understanding of cryptography, what hope is there for everyone else? Could I write a book that could help to demystify the role of cryptography, not just for professionals such as Gordon Corera, but for the public at large?

Then in 2016, I was asked to contribute some lessons on cryptography as part of a Coursera MOOC (Massive Open Online Course), designed to introduce the wider public to information security. These lessons consist of six ten-minute videos. Could I present cryptography in just one hour to a general audience? I thus developed a concise six-segment narrative that explained the role cryptography plays in cybersecurity. These lessons have proved popular, with over 100,000 unique visitors and almost 30,000 enrolments, and provided the launch pad for a new book.

So what, in essence, is this new book about? Well, it's not a textbook. In a UK bookshop it will belong on the shelves associated with "popular science". The aim of the book is to open readers' eyes to the critical role cryptography plays in supporting our everyday lives. It examines why we need cryptography in cyberspace, what it does, how we use it, and what its limitations are. One of main purposes of doing so is to use the explanation of cryptography to provide readers with a more profound perspective on their own personal security when they are operating in cyberspace. I also want to help readers adopt a more informed position about the post-Snowden world. The book thus discusses the role cryptography plays in the wider social debates concerning how society should balance personal freedom with control of information.

Early in the writing process I had dinner with a former colleague. When I told him I was writing a popular science book about cryptography he replied, "Why bother? Didn't Simon Singh already do that?" Well, yes, he did. The Code Book is a very accessible 1990's book about cryptography, which many of you may have read. But The Code Book takes a much more historical perspective and predates the rise of cyberspace as a place where we live our everyday lives. The Code Book essentially presents cryptography as cool science with an interesting past. I have chosen to present cryptography from the perspective of our contemporary need for security in cyberspace. I see The Code Book as complementary, and certainly not a direct rival. I would love all The Code Book fans, however, to read my book and see cryptography in modern light.

Writing any type of book is not a fast process, but writing a "trade book" of this type has been painfully slow and quite different to academic publishing. I started writing in autumn 2016 and developed the first draft over the subsequent twelve months. I soon learned that getting visibility with publishers requires having an agent. After a false start, I was very lucky to make contact with Peter Tallack at the Science Factory, who helped me prepare a formal book proposal in autumn 2017. By spring 2018 I had a draft that I was willing to share, and several friends and colleagues, including Fred Piper, provided valuable feedback. In autumn 2018 Peter took the book proposal to market and I secured conversations with several publishers, eventually formalising a deal with WW Norton, an independent employee-owned publisher in New York. The book then journeyed through the pre-publication process in 2019, including editorial review, copy-editing, proof-editing and the thorny issues of title and cover design. I spend much of my working life "red-penning" student manuscripts, but in 2019 I got a healthy dose of my own medicine!

The last words were tinkered with in December 2019 and the book is finally due to be published in May 2020 in the US, the following month in the UK. There's even a Chinese and a Korean edition already commissioned, but I'm certainly not offering to proof-read either of them. I hope the book will achieve its aims, but only readers can deliver the verdict on that.

CRYPTOGRAPHY
THE KEY TO DIGITAL SECURITY, HOW IT WORKS, AND WHY IT MATTERS

# WELCOME

This year we welcome three new lecturers to the ISG. They are: Systems Security Researcher - Darren Hurley-Smith, Threat Detection Scientist - Jassim Happa and Researcher in Cryptography - Rachel Player.

We asked them three questions to find out a little more about who they are, what motivates them in their work and what piece of advice they have for junior academics working their way towards their first lectureship. Here's what they had to say:

What motivates you to be an academic and how does that play out in your day - to - day working life?

Jassim:

I've always enjoyed learning, and being an academic enables me to continue learning in life 'as a job'. I use my enthusiasm for learning to continually try out new things in my research. I also love having my understanding of topics be challenged by different perspectives from others, so I gain even further insights about any particular topic. Being an academic also grants me the freedom to research topics I want in a way that I suspect wouldn't be possible in most industry jobs.

Darren:

As cliched as it sounds, the exploration of the new is my primary motivator in my academic work. I enjoy finding novel weaknesses in trusted systems, particularly at the hardware level, and engineering solutions to those problems. Building more secure systems is rewarding and the initial discovery and communication of flaws is exciting: the thwarting of potential security threats has a romantic quality which invigorates what can otherwise be a dry procedural process. If I had to summarise my academic motivation in a phrase, it'd be "Security, for the end user, should be a given. Trust is built through the incisive and uncompromising criticism of current approaches, and the development of new systems that can function independently of end user technical ability and understanding."

As a result, my research combines analysis of real-world systems with supporting simulations which explore precisely how easy it is to introduce biased data into random number generator output, while evading detection by statistical testing methods employed by manufacturers and certification bodies. I integrate this self-critical approach to systems and security testing into my teaching, where I like to encourage students to identify not only the correct tools, but the limits of those tools in identifying potential security threats.

Rachel:

So many things! Firstly, I love meeting new people and so being able to (in usual circumstances!) travel frequently to conferences and events is a great benefit of being an academic. I had never taken a long-haul flight before my PhD whereas in the last year alone I presented my research in the US and New Zealand.

Secondly, being a researcher in an academic setting gives a great sense of freedom. Most obviously, it allows me to set a research agenda based on my own interests. In addition, it allows me the flexibility to contribute to the community. For example, I am able to participate in standardisation efforts (something I greatly enjoy).

Thirdly, I find teaching to be a very fulfilling part of the job. At Royal Holloway, and in the ISG in particular, we benefit from the collegial atmosphere and close-knit community, which makes it easy to connect with students. I try to be as approachable and flexible as possible in order to help students achieve their goals.

If you were to pick one role model for your academic work who would that be and why?

Jassim:

I view Socrates, Plato and Aristotle as key role models. While I could pick any one of them and list their individual contributions, I think it's good to view them as a trio. Individually, they had different (sometimes incompatible) views in philosophy, but many of their contributions led to important progress in society and sciences. When viewing them as a trio, we quickly see that there is often no single "right answer" to many research challenges. Instead, different perspectives are vital, and, in many ways, one's research always builds on prior research.

Darren:

My PhD supervisor, Dr Jodie Wetherall, was highly influential during my Bachelor's studies and encouraged my initial interest in pursuing research as a career. His patience and mentorship added much needed stability to my early years as a PhD student. A shared interest in engineering, systems analysis and 'the art of the acronym' helped to form a lasting research partnership after I moved on to my first post-doctoral role at the University of Kent.

There, Prof. Julio Hernandez-Castro encouraged me to take my research further, and introduced me to the rewarding world of inter-disciplinary research, namely the economics of cyber-crime and cyber-security. His enthusiastic and encouraging demeanour, and impressive command of mathematics and cryptography acted as an example to me as I transitioned from aspiring researcher to early career academic.

Rachel:

I would have to say Kristin Lauter, although this is cheating a bit in terms of "in academia", since her main role is in industry as a Partner Research Manager at Microsoft Research. I hasten to add that she is also an Affiliate Professor at the University of Washington! While her research contributions in cryptography are vast, the main reason I admire her is because of her efforts to promote women in mathematics. For example, she is a co-founder of the Women in Numbers community, which organises conferences to facilitate networking and research collaborations for women number theorists. Kristin takes every opportunity to encourage and promote talented junior researchers, and I would like to be the same kind of leader.

Given where you are now professionally, what would you have told your 2017 work-self?

Darren:

Ultimately, the tempo of your research is in your own hands. Rejections, waiting periods and disruption may seem to rob you of agency, but there's always a new idea and direction you can pursue while others sit in the waiting room of peer review. You'll be happier and more productive filling any 'dead air' with all those small questions that your previous projects left unanswered, or investigating a viable new line of thinking while waiting for substantive feedback that will feed into your current main project(s).

Rachel:

Regular readers may remember that in 2017 I was featured as the student profile in the ISG newsletter and I am not sure I would have believed I would already be a lecturer three years later! Since 2017 I've had the opportunity to visit several other institutions for research visits, as well as spending time elsewhere as a postdoctoral researcher. One thing I have realised is that being part of a vibrant research community is key: it is motivating, and more fun, to be able to readily share ideas. The collaborative ethos we have in the ISG was something I took for granted as a PhD student, but ended up being one of the key reasons why I (like so many before me!) wanted to come back.

Jassim:

There are many directions we can go in academia (career-wise). I think it's important to strike a right balance of what's important for you when juggling between activities. Knowing what that right balance is though, is challenging. I guess what I would have told my past self is to find ways to learn what matters to you, so you can prioritise academic activities better.

# THE IMPACT OF QUANTUM COMPUTING ON MOBILE SECURITY

Chris Mitchell

> Professor ISG

In recent years the impact of quantum computing on cryptographic systems has been widely discussed. While there is no general agreement that large-scale, general purpose, quantum computers will ever be built, a huge development effort nevertheless continues. Such computers would have a major impact on the security of many of today's cryptographic systems, since algorithms for quantum computers have been devised which impact both symmetric and asymmetric cryptography.

- Shor's 1994 algorithm has a major impact on the security of all widely used asymmetric algorithms – all schemes based on the difficulty of factoring large integers or computing discrete logarithms (including elliptic curve schemes) will be rendered insecure for feasible key lengths.

- Complementing this, Grover's 1997 algorithm affects the security of all symmetric algorithms, albeit much less severely. All symmetric algorithms will in effect have their key lengths significantly reduced (in principle halved, but in practice the reduction will be somewhat less). Given the degree of uncertainty involved, in line with established practice we use the conservative estimate that, if a quantum computer is available, a 128-bit key will be roughly as secure as a 64-bit key is today, i.e. it will be insecure.

So, for every major application of cryptography, a careful review of the impact of quantum computing is needed. A review should assess which parts of a system are vulnerable if a quantum computer becomes available, and what the impact would be; it should also consider how long it would take to upgrade the cryptography, including the time required to update the specifications, produce replacement implementations, and replace all deployments. The total time could be very considerable, depending on the domain. For example, credit cards have a typical lifetime of three-five years, so replacing them all could take a decade or more (given the need to also replace the infrastructure supporting their use).

Mobile phone security has relied on cryptography since GSM (or 2G for the 2nd generation of mobile), first deployed in 1991. 5G is the latest generation mobile system, and 5G technology is now being deployed. Mobile systems are very widely used worldwide, and 5G looks set to become even more closely integrated with society; 5G security is thus very important.

## A STUDY

A recent study (see arXiv:1911.07583) gives a detailed review of the operation of 5G security, and considers the ramifications of the post-quantum (PQ) era on its effectiveness. This study also gives a series of recommended changes to the 5G security, designed to minimise both the practical impact of PQ-era attacks and the cost of implementing the changes.

The changes focus on the use of 128-bit keys, the security of which will be at risk in the PQ era. In particular, the long-term USIM key is currently only 128 bits long. This is used within the USIM to derive two 128-bit keys; they are exported to the phone, which uses them to derive a range of 128-bit keys used to protect data and voice sent across the radio interface – how keys are derived depends on whether the network is 3G, 4G or 5G, although the USIM works in exactly the same way regardless of network type. In addition, asymmetric encryption is used to provide user identity privacy – a standardised algorithm (which is not ‘PQ secure’) can be used or the USIM issuer can choose a proprietary algorithm.

## MAIN FINDINGS

Unless quantum computers become very cheap and ubiquitous, a few relatively minor changes will ensure that the security impact of the PQ era is minimal. The recommended changes are in three groups, implementable over different timescales. The first group of changes upgrades the security of 3G and 4G networks, as well as 5G.

## INITIAL CHANGES TO SYMMETRIC CRYPTOGRAPHY

These changes should be implemented as soon as possible, and can be achieved without impacting any deployed infrastructure or mobile terminals. They involve modifying the standards to allow 256-bit (as well as 128-bit) long-term secret keys to be stored in the USIM, and allowing 256-bit inputs to the functions using this USIM key; examples of recommended functions using a 256-bit USIM key are also needed. Importantly, a set of candidate functions of this latter type has already been specified, namely the Tuak functions (see 3GPP TS 35.231).

## ASYMMETRIC CRYPTOGRAPHY CHANGES

These changes should be made once PQ-secure asymmetric encryption algorithms are standardised, perhaps in two-three years’ time. This means adding guidance on the adoption of proprietary PQ-secure asymmetric encryption schemes for protecting permanent user identifiers. Further, at least one such scheme should be included in the relevant 5G standard, and its adoption by operators encouraged.

## LATER CHANGES TO SYMMETRIC CRYPTOGRAPHY

These changes involve switching to 256-bit cryptography throughout. This will require changes to the operation of mobile terminals and mobile networks, but not to USIMs; indeed, the current phone/USIM interface can stay unchanged. For smooth migration it should also be possible to specify the changes to allow parallel use of 128-bit and 256-bit keys. New 256-bit symmetric encryption and MAC functions will be needed, although the 4G and 5G key derivation architectures, which use the two 128-bit keys output by the USIM as input, already generate 256-bit keys; they are currently truncated to work with 128-bit functions. In fact, work is already under way within 3GPP to see what, if any, new functions need to be defined for such a move (see 3GPP TR 33.841).

## CONCLUSIONS

The changes necessary to make 5G completely ‘post-quantum secure’ are modest in scope and appear to be eminently realisable in a phased way. Moreover, because the need for a future switch to PQ-security has been anticipated in the 4G and 5G designs, much has already been done, notably the use of 256-bit keys in the key derivation chain, specification of the Tuak functions, and 3GPP TR 33.841. Standards writers, network infrastructure and handset manufacturers, and network operators are encouraged to complete the changes. The sooner the necessary changes are made, the smaller the threat will be when the PQ era dawns.

# BEHAVIOUR CHANGE: CHALLENGES FOR INFORMATION SECURITY

Konstantinos Mersinas

> Lecturer ISG

In recent years, attention in information security has been gradually turning towards human aspects as academia, government and industry are recognising the importance of psychological and behavioural factors [1]. However, as Bada et al demonstrated [2], traditional security awareness training campaigns are ineffective in unlocking the full potential of humans as a line of defence. Thus, security behaviour change remains an open question and security practitioners grapple with the challenge of enabling individuals to understand, adopt and manifest these desired behaviours.

The majority of literature on behaviour change originates from the health sciences. Meta-analyses from studies looking at, for example, alcohol consumption, smoking, poor nutrition or lack of exercise, show that behaviour interventions can be effective. However, behaviour change is still difficult to achieve even when people face possible life-threatening risks due to such behaviours. Designing interventions to successfully changing cyber security behaviour is even harder!

## How can we persuade individuals to change their security behaviour?

We can think of a behaviour change approach as having a messenger, a message and a receiver. The message includes a threat and a suggested solution to be accepted or rejected by the receiver. To encourage particular behaviours and responses, interaction designers sometimes deploy Aristotle's three methods of persuasion [3]: appealing to the audience's emotion (pathos), appealing to the audience's reason (logos), or using the  speaker's credibility and character (ethos). These methods can be used to different effect. For example, a messenger might choose to convey a security message appealing to the receiver's reason, if they believe that the receiver will invest the time to make choices between alternative courses of action. There are limitations to this approach, especially as people, regardless of their security expertise, might make subjective, sub-optimal decisions. So, the messenger might also try to appeal to the receiver's emotions, if the messenger believes that this is the basis on which a course of action will be chosen. Finally, Aristotle posits that 'who the messenger is' might also be  influential. Messages designed for behaviour change must therefore be both carefully constructed and delivered.

Various psychological theories and behaviour change models exist ([4], [5], [6]), but there are not many practical, effective implementations. Instead, psychological solutions rely on mass media or education campaigns often delivered on ad-hoc basis. But since behaviour change is shown to depend on, for example, culture, age and individual risk attitudes, solutions need to be customised for the individual as well as for the setting.

## So, why is behaviour change hard?

There are a number of challenges related to behaviour change:

1) Identifying what constitutes desirable behaviour in information security. 'Following security policies' is perhaps not a constructive way forward and understanding which behaviours work is better. For example, Witte [5] suggests that the desired reactions to communicated threat messages are cognitive responses, rather than emotional ones.

2) Defining 'rationality' and emotional appraisals. These notions are not straightforward, especially in an information security context.

3) Selecting and weighing the behavioural intervention variables to be modelled. According to Rogers [4], the perceived level of threat, along with the individual's perceived efficacy to cope with this threat, are the main predictors of whether people take protective actions or not. Additionally, Fogg [6] proposes the factors of motivation, appropriate triggers, simplicity of solutions, peer pressure and social acceptance.

4) Including security culture as an 'environmental' factor in the equation. Considering situational circumstances which might affect message acceptance, but modelling them to a sufficiently adaptable level.

## Finally, what constitutes 'appropriate' interventions?

Not only is behaviour change hard but, even when successful interventions are discovered, ethical issues often emerge that challenge the deployment of these interventions. In particular, ethical issues arise with behavioral interventions on at least two levels. In the first instance, successful behavioural interventions need to be shaped by an individual's characteristics. The messenger needs to have access to these characteristics as it is the individual's perceptions, skills and attitudes that influence which security messages the individual regards as acceptable. However, the mere act of 'customisation' might threaten privacy. The environment is important too. For example, in an organisational setting where message receivers are employees, data protection compliance results in a certain level of monitoring which is (at least legally) acceptable. However, ethical acceptability of monitoring of public online social media, although an established law enforcement procedure, is potentially a different matter if vulnerable groups such as children are monitored. Importantly, tech giants increasingly invest in behavioural data collection (even if only meta-data). The purpose of this is mainly targeted advertising and profile-building, although through aggregation and analysis this can lead to behavioural predictions for consuming, voting and practically any human activity [6]. So, the digital landscape might already be 'privacy-hostile', and thus, acceptability of additional data collection, even for well-intentioned behaviour change, might be problematic.

In the second instance, there are ethical considerations with the type of interventions themselves. For example, there is a long history of advertising-industry 'tricks' for increasing consumption. That is, there exist methods which drive individuals' behaviour without them being aware of this process. Should we, therefore, allow for interventions which use conscious and non-conscious mechanisms to nudge individuals' security behaviours?

In conclusion, there is no 'royal road' to security behaviour change and we are far from envisioning relevant standardised 'best practices'. We are only scratching the surface of a complex problem, but solutions, if any, will most likely emerge together with a further understanding of human behaviour.

### References

[1] Kenneally, E., Randazzese, L. and Balenson, D., 2018, June. Cyber Risk Economics Capability Gaps Research Strategy. In 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-6). IEEE.

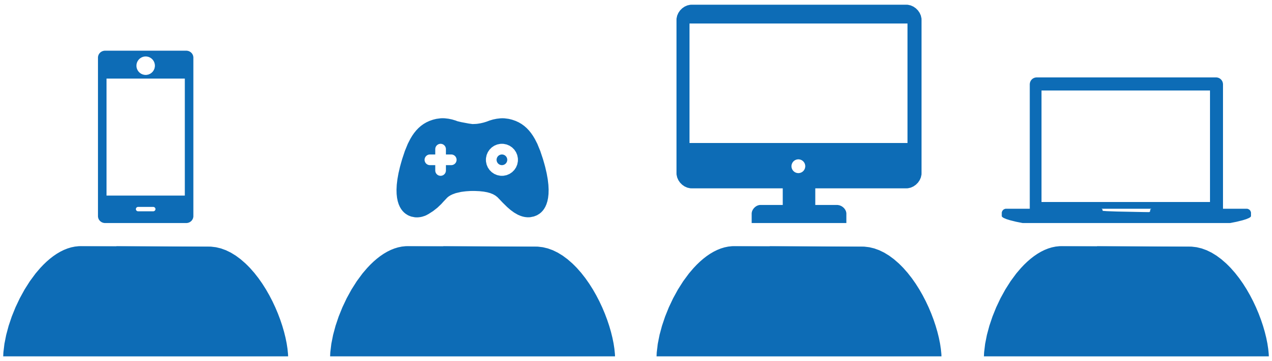
[2] Bada, M., Sasse, A.M. and Nurse, J.R., 2019. Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

[3] Buchanan, R., 2001. Design and the new rhetoric: Productive arts in the philosophy of culture. Philosophy & rhetoric, 34(3), pp.183-206.

[4] Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1), pp.93-114.

[5] Witte, K., 1998. Fear as a motivator, fear as inhibitor: Using the EPPM to explain fear appeal successes and failures. The Handbook of Communication and Emotion.

[6] Fogg, B.J., 2009, April. A behavior model for persuasive design. In Proceedings of the 4th international Conference on Persuasive Technology (p. 40). ACM.



## DOING WHAT YOU CAN IN A TIME OF CRISIS

Lizzie Coles-Kemp

> Professor ISG

For the last twelve years, I have written sporadically for our newsletter about my work with under-served and marginalised communities. The work stretches back to 2008, when I started working on a UK Research Council project called Visualisation and Other Methods of Expression (VOME). This project sought to work with communities around the country to better understand the security implications of the UK government's "Digital by Default" programme. The focus of VOME was to work with marginalised and under-served communities to better understand what risks they associated with accessing on-line essential services such as housing and welfare services and to co-develop approaches to managing those risks.

Through VOME, we developed new knowledge about the importance of kin and friendship networks when making decisions about sharing information in on-line settings. We learned about the roles such networks play in creating a circle of trust in which people can both solve access problems and make access decisions. It was in this project that we started to realise how the social, economic and political context in which someone accesses a service both shapes and is also shaped by on-line behaviours and practices. For example, the withholding of information when using essential services is a practice that often stems from a person's perception of the service provider as hostile or a threat actor.

In the case of essential services, where the service provider often needs to build and maintain a positive relationship with the service user, non-compliance with security policies can put that relationship at risk. For example, our research found that it was not uncommon that a person accesses a service through someone else, a type of informal social proxy. This third party was often a family member or a friend. In many cases, this arrangement was positive and provided a safe and reliable form of access for a vulnerable person. However, such access also had the potential for being an avenue for abuse and the service provider typically had no means of knowing the difference between supportive and abusive assisted access. Whilst technology can be developed to respond to this problem, our research showed that the most effective forms of response were often social. Much of our research therefore has focused on supporting forms of safe relationship building, ways of messaging security concerns and informing security practices that are actionable in situations where there is limited access to the internet and where standard on-line security choices are not always available.

The COVID-19 pandemic has meant support for marginalised and under-served communities has come under pressure as never before. Within the space of a week, essential services offering support for such communities had to largely be moved on-line and many vulnerable people had to turn to on-line services as their sole means of accessing that support. Whereas before the pandemic, vulnerable people could go to a library or a community centre to get help with accessing essential services, the lockdown policy meant that they had to manage access on their own in home environments that might be volatile or chaotic with potentially limited internet access. At the same time, entirely new groups of people needed to start accessing digital essential services, and new types of vulnerable groups therefore began to emerge.

The ISG is part of the Digital Economy funded network, [1] Not-Equal. The network is funded to bring together research and community action to produce practical responses to problems of inequality that arise from the digitalisation of society and the economy. Our work in Not-Equal is to co-ordinate the Digital Security for All stream and our immediate COVID response  in this stream has been to ensure, as far as possible, that the groups we work with have access to e-safety information. We have also been flagging up issues and challenges as well as possible responses to the relevant social inclusion and e-safety teams across UK government. Our focus during this time is to support community groups to safely provide their services to vulnerable groups. We are now preparing for post-lockdown support provision and are working with Not-Equal to identify where support for community groups will be most needed and what form that support should take. At the time of writing, we are still only part-way through the consultation but initial feedback shows that community groups are reporting a need for i) more reliable and better quality internet access, ii) on-going digital safety and computer security support, iii) better ways of trust building and sustaining relationships  on-line with vulnerable people and iv) ways of identifying when vulnerable people need help and support.

In meeting these challenges, safety and inclusivity – both for those providing and those receiving the support – will be key. Whatever we can offer will only be a fraction of what is needed but we hope to be able to put to good use  the knowledge and know-how that we have gained in our social research projects over the past 12 years.

[1] https://not-equal.tech/

# THIRTY YEARS* OF THE INFORMATION SECURITY GROUP

Keith Martin

> Professor ISG

The year 2020 marks the 30th anniversary of the Information Security Group at Royal Holloway. Or does it?

*OR MAYBE 36 OR MAYBE 28

we are 30

## False Dawns

It could be argued that 2020 is the 36th anniversary of the ISG. In 1984 the University of London was undergoing a major restructure which involved closing a number of its smaller Colleges. This saw a number of key academics join Royal Holloway, including Fred Piper and Peter Wild to the Department of Mathematics, and Thomas Beth, Dieter Gollmann and Chez Ciechanowicz to the Department of Computer Science. These were not independent appointments, since Fred and Thomas shared an interest in cryptography, and Fred had persuaded Thomas to take up the role of Chair of Computer Science. Shortly afterwards Fred founded Codes & Ciphers Ltd., primarily to use consulting projects to connect academics to relevant issues arising in government and industry. There was thus almost an ISG in 1984, except that the following year Thomas returned to Germany, taking Dieter with him. By 1989 Chez had also departed for Zergo/ Baltimore.

Another candidate foundation year for the ISG is 1992. This was the year that the MSc in Information Security was launched, a programme which has underpinned the growth and success of the ISG. The 2008 white paper The Information Security Group: A Brief History argues that 1992 `in some sense might be argued to be the starting point for the ISG'. So 2020 is the 28th anniversary of the ISG, right? What happened in 1990?

The strongest case for the ISG foundation year is 1990. This is the year that Fred, then Head of Mathematics, persuaded Chris Mitchell to leave Hewlett Packard and take up a position as Professor of Computer Science at Royal Holloway. Chris recalls that there were several reasons why he made this move. `One major reason was the desire to work more closely with Fred and Peter, bearing in mind that Fred was my PhD supervisor (1975-79) and I had known Peter as a fellow PhD student, friend and research collaborator since 1976. I also wanted more control over the direction of my research.'

From here, things started to snowball. Dieter Gollmann, now a Professor at Hamburg University of Technology, recalls that in late 1989 he met Chris at the IMA Conference in Cryptography and Coding. `Chris told me that he had been appointed Head of Department of Computer Science at Royal Holloway, a Senior Lectureship would be advertised, and would I please consider applying. My first stay at Royal Holloway had been much too brief, so I did and got the job.' Dieter was followed by Sean Murphy, who was a joint appointment with Mathematics, and Kwok Yan Lam, who is now a professor at Nanyang Technological University in Singapore.

It wasn't just the intake of people arriving in 1990 that makes this the best candidate foundation year for the ISG. It turns out that 1990 was the year the ISG was named, thanks to Chris Mitchell. `I arrived at Royal Holloway in March 1990, and Fred and I came up with the name very soon afterwards as a way of creating a cross-departmental entity, which seemed the natural thing to do given we were spread across two departments but yet wanted to make it clear that we worked together as a single research group. In fact, for what it's worth, I think I devised the name - Fred wanted to call it the data security group, but information security group sounded better/more modern to me.'

## The Mastermind

There might be doubts about exactly when the ISG was formed, but there are none about whose brainchild it was. In the words of Peter Wild, `Without Fred the ISG would not have been established. It was his vision and he gathered the personnel to make it happen. Through his association with industry and his insight of how the field was developing,

Fred recognized the need for a contribution by academia to train information security specialists to fill the growing demand for expertise in the area. He persuaded the College to make the appointments and to establish the MSc. He was the driving force, the negotiator and the leader.' Chris more succinctly states, `Fred was the éminence grise.'

### Birth of the MSc

The creation of the MSc was the first major project of the new-founded ISG. While the ISG has always been about much more than the MSc, the programme has had an enormous influence on the personnel that the ISG has hired and the international reputation of the ISG. Chris remembers that the planning for this innovative programme, the first of its kind in the world, was very much a team effort. `As a team, we came up with the original structure and syllabuses for the main courses based on our own experience and knowledge of the area. We then ran them past our friends and collaborators in industry and adjusted them based on the input we received.' These friends and collaborators included some of the most influential players in what was then a relatively fledgling cyber security industry. A 1991 planning document for the MSc credits the significant influence of Henry Beker (founder of Zergo Ltd and Chairman/CEO of Baltimore Technologies, a pioneering digital security company), Donald Davies (computer scientist and former NPL researcher, widely credited as one of the inventors of packet-switched networks) and Mike Walker (then of Racal Research but soon Vodafone, and later to play a lead security role in the new mobile telecommunications industry).

The same planning document also identifies several reasons for the three-hour block-teaching model that has stood the test of time. This wasn't just to support part-time students (who were correctly identified from the outset as a key market for the programme), but also to `enable a considerable proportion of the material to be taught by external (commercial and industrial) lecturers.' This was both necessary, as the ISG was small and did not then have the full breadth of expertise to deliver the entire syllabus, but also desirable, as it exposed students to frontline information security professionals and helped to bring this early security community together. To a more limited extent, this practice continues today.

For Chris the birth of the MSc was a very rewarding time. `These were happy days - we were putting everything together quickly, and getting really important stuff done. What makes me a bit sad is how much more difficult it is today to get things done because of the greatly increased bureaucratic overhead. I hate to think how much more work it would be in today's university environment to develop and put on such an innovative new degree programme. I don't remember it being difficult back in 1990 - we knew what we were doing, so we were just allowed to do it.'

### Information security in 1990

So what were the pressing information security issues back in 1990? Remember that there was no World Wide Web and in 1990 mobile phones still vaguely resembled bricks.

Peter remembers the state of the general information security environment, which indicates exactly why the time was right for the formation of the ISG. `Information Security prior to 1990 had been dominated by government and the military, but its importance to commerce and industry had only recently emerged. Initiatives were being taken to transform ad hoc approaches to more systematic ones, so that information security could be designed, implemented and managed in a more reliable way. The field had moved into the public domain.' `Security was very much a niche subject then,' recalls Chris. Specific industries (banking and telecoms, in particular) and governments had major security concerns and invested significantly in security technology. However, because the Internet was not something most people used, and mobile data was still in the future, the threat from connectivity to everyday users simply didn't exist. Critical infrastructure was also not connected as it is today, so again the threats simply weren't there. However, PCs were already in widespread use and there was a growing threat from, and awareness of, malware, even if the main attack vector was exchange of floppy disks!'

Kwok Yan Lam reflected on the types of security problem that researchers were concerned with back then. `Information security was not a big field then, but it was growing. People were mostly working on crypto (PKI was considered new), authentication protocols (Kerberos was big), formal methods for protocol verification (e.g. BAN logic and GNY logic) and covert channel analysis. This was all before the e-commerce and HTML browser era, so the pressing need was really to translate the academic results into something useful in the real world.'

### Standing the test of time

It is worth reflecting on just how visionary the early MSc syllabus design decisions were. After all, the core programme structure planned in 1990 remains almost the same today.

Dieter is not surprised. `That's because I was the Programme Director when we did the final planning,' he jokes. `More seriously, the fundamentals of IT have not changed: organisations use computers connected by networks to help them to achieve their mission. These resources and the people using those resources need to be managed, the computers and the networks need to be secured, and sensitive data need to be protected. For the latter, cryptography is sometimes the only option. This is the justification of the four core modules of the MSc – both then, and now.'

But did anyone predict just how successful the MSc would prove to be? Peter certainly didn't. `Even as the number of students grew it was always a surprise to me each year that the number had increased again - the growth was amazing.' Chris recalls modest ambitions of what success might look like: `We speculated that 15 or so students a year would be a good outcome.' Similarly, back in 1990 Dieter was not sure how important the field of information security was going to become. However, `GSM and opening the internet for general (and thus commercial) use came along later and totally changed the game.'

But Kwok Yan Lam was not so surprised. He was sure that information security was going to be of enormous importance, which motivated his choice of career. `I firmly believed in this when I first listened to Fred Piper and Tom Beth back in 1984. At that time, I believed eventually every phone would have a crypto engine – it became true when the GSM phone was invented.'

## Thirty years later

Thirty years is a good length of time over which to reflect on changes and successes.

Technologically much has changed, and Dieter was challenged with considering what he regards as the most surprising development over those 30 years. `Probably the smartphone. A device without a keyboard that is as powerful as a supercomputer from 1990. It has brought about applications I would not have dreamed about in 1990 and it keeps turning the user into the manager of a security relevant device. The smartphone has also created new communities of software ('app') developers blissfully unaware of software security lessons learned in established fields. One might add to the list of surprises that Microsoft is today a leader in software security!'

What about successes for the ISG? Looking back, what makes the founders most proud?

For Peter, it's `the high stead students hold in their education and the ISG itself, and how willing they are to maintain contact with the ISG and continue to contribute to it. One might say that the ISG is really not just the staff but the whole community of staff and students, past and present.' For Chris, it's `establishing the MSc and maintaining it as one of the leading offerings in the area. I believe it has been hugely influential on security teaching at both masters and undergraduate levels. Of course, we have established our research reputation as a group over several decades, but there were already many other security research groups around the world, even in 1990. However the MSc, I believe, was the first of its kind in the world.' For Dieter it's the legacy of an influential international alumni community, noting, for example, that in the Korean information security community ISG graduates are known as The Royal Family!

## What about 2050?

So will the ISG be around in another 30 years? Kwok and Dieter were brave enough to hedge some bets. `As long as there are people, there will be security issues,' observes Kwok, `but the manner in which they manifest themselves in 2050 will depend on how people interact. I believe the ISG will still be very relevant, but I am confident we will not be using the term cyber security in 2050!' For Dieter, `Thirty years is far enough into the future that I will hardly have to eat my own words! I see the demand for people with a good understanding of security growing. The bigger question is probably whether universities, and MSc programmes, survive as a means of education. If they do, then the ISG will surely have its place.'

## The last word

There is only one person to turn to for a last word about the ISG's 30 (or maybe 36 or maybe 28) years. For Fred Piper, the ISG has always been about people.

`Since it's foundation members of the ISG have all been of a high standard and I am very proud of what they have achieved.'

# WRITING FOR PUBLICATION: AN OPPORTUNITY FOR GRADUATE AND POSTGRADUATE STUDENTS

Siaw-Lynn Ng

**> Senior Lecturer ISG**

The ISG has a long tradition in cyber security research, and is one of the largest academic cyber security research groups in the world. Along with academics and research assistants, there is a large group of postgraduate research student, working on topics ranging from cryptography to cyber economics. In addition, the ISG has a proud tradition of information security education. Founded in 1992, the ISG's flagship MSc Information Security masters degree programme has now produced over 4,000 graduates from more than 100 countries in the world.

Besides publications in peer-reviewed journals and conferences, we provide an opportunity to communicate new ideas and insights more informally to other security professionals. This also allows graduate and postgraduate students to improve their technical and communication skills, to establish them as an expert in their fields of study, and to influence the development of those fields. These articles are written mainly for security professionals, and give general introductions to topics of interest, or provide analysis of current issues in cyber security, without assuming that readers have an extensive mathematical or computer science background.

One venue of online publication is the Infosecurity magazine (https://www.infosecurity-magazine.com/) Next-Gen Infosec series. These are very short blog-style articles from postgraduates for a readership of IT security practitioners. In one recent article PhD student Amy Ertan discusses, topically, the shift to virtual webinars as a tool for cyber security inclusivity. There are a few more articles in the pipeline, on the topic of human aspects of cyber security, as well as articles published in previous years by our PhD and MSc students.  These articles are written in a style that makes them accessible to everyone, and I would recommend them to anyone interested in various aspects of information security.

Another publication venue of these articles is the Computer Weekly ISG MSc Information Security thesis series. This is a series of informative leading-edge articles distilled from outstanding MSc projects which best present research in an area of information security of interest to information security managers and professionals. This year there are seven articles on topics ranging from the future of autonomous vehicles to the security of the devices many of us use every day.

We rely on USB flash drives as an easy way to transfer data. However, the use of these devices carries its own security risk, from data theft to the transfer of malware.
Daniyal Naeem (supervised by Keith Mayes) outlines a strategy to identify what security attributes such a system must have, and compares the new strategy with established methods, in the article “An Enhanced Approach for USB Security Management”. Another device that sees pervasive use is mobile phones. In order to cope with increasing performance requirements, mobile devices must get more powerful, and the optimisation of hardware sometimes accidentally creates security vulnerabilities. In “Rowhammer: From DRAM Faults to Escalating Privileges”, Jan Kalbantner (supervised by Konstantinos Markantonakis) describes a widespread attack based on a hardware vulnerability, and discusses what paths future research might take to mitigate variants of this attack. Connected devices also suffer from malware infection and one of the defences against this is the detection of malware using clustering algorithms. Rebecca Merriman (supervised by Daniele Sgandurra) studies the accuracy of such algorithms in the article “A Novel Approach to Clustering Malware Behaviour to Improve Malware Detection” and examines factors that might affect the results.

In “Man Proposes, Fraud Disposes”, Tony Leary (supervised by Geraint Price) dissects the 2017 incident where the ‘WannaCry’ ransomware infected 32 National Health Service trusts in England and discusses the principal causes. Since it is not likely that we can completely mitigate the threat of attackers getting into our networks, Felisha Mouchous (supervised by Daniele Sgandurra) proposes a threat modelling and security testing framework in “Purple Team Playbook: Threat Modelling for Security Testing” to allow organisations to leverage existing data to identify gaps in defences and understand threat actor behaviour. Organisations may also turn to cyber insurance to cover a portion of their enterprise risk. In “Lessons on Catastrophe – Differences and Similarities between Cyber and Other Forms of Risk”, Rob Champion (supervised by Carlos Cid) summarises high level findings on a practical model that could be used in lieu of actuarial data.

One exciting trend is the emergence of connected and autonomous vehicles.
In “Trusting Connected and Autonomous Vehicles to be Secure: The Long Road Ahead”, Juliet Flavell (supervised by Paul Dorey) discusses some of the requirements, constraints and challenges, and areas of uncertainty in this technology, while in “Driverless Vehicle Security for Military Applications”, Nicola Bates (supervised by Raja Naeem Akram) discusses whether the civilian autonomous vehicle security frameworks are suitable for military logistics autonomous vehicles. Nicola examines the threats considered from the point of view of an enemy so as to identify critical weaknesses and countermeasures.

These MSc projects are re-written in collaboration with the individual’s ISG project supervisor as accessible short articles for a general professional readership and published online at www.computerweekly.com. As they are published by Computer Weekly we announce them on our website https://royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/computer-weekly-search-security-awards/. Note that these articles are distilled from the full project reports and necessarily omit many details. Readers interested in particular articles can obtain the full reports from the ISG website (https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/).

# CRYPTOGRAPHIC SECURITY PROOFS AS DYNAMIC MALWARE ANALYSIS

Martin R. Albrecht

> Professor ISG

RSA encryption with insecure padding (PKCS #1 v1.5) is a gift that keeps on giving variants of Bleichenbacher's chosen ciphertext attack. As the readers of this newsletter will know, RSA-OAEP (PKCS #1 v2) is recommended for RSA encryption. How do we know, though, that switching to RSA-OAEP will give us an encryption scheme that resists chosen ciphertext attacks? Cryptography has two answers to this. Without any additional assumptions the answer is that we don't know (yet). In the Random Oracle Model (ROM), though, we can give an affirmative answer, i.e. RSA-OAEP was proven secure. Indeed, security proofs in the ROM (and its cousin the Ideal Cipher Model) underpin many cryptographic constructions that are widely deployed, such as generic transforms to achieve security against active attacks and block cipher modes of operation. This article is meant to give some intuition about how such ROM proofs go by means of an analogy to dynamic malware analysis.

The thought experiment in a typical (game-based) cryptographic proof starts by assuming that there is indeed an adversary that breaks the security goal of our cryptographic construction. For example, assume this adversary can decide if some message A or some message B was encrypted in ciphertext C. We are not even asking the adversary to decrypt C but we are merely asking it to decide which of two messages of its choosing we encrypted. If it cannot even do that, it cannot decrypt or learn anything about the underlying plaintext of a ciphertext. So this is the adversary's goal: to distinguish. Next we need to decide what capabilities our hypothetical adversary has. Here, let's consider chosen ciphertext security. The adversary gets to ask for decryptions of any ciphertexts it wants except for the "target" ciphertext C we are challenging it to make a distinguishing decision about. We are taunting the adversary: "We're giving you the ability to decrypt anything you like except this one ciphertext but you still cannot decrypt it. In fact, we let you choose two messages A and B and we will encrypt one of them for you, you won't even be able to decide which one we picked"; yep, cryptographers taunt algorithms. This is known as IND-CCA security in cryptography and the standard security notion aimed for and achieved by encryption schemes.

Now to illustrate how these proofs proceed, we will think of the adversary as a piece of malware. To analyse it we are going to put it in a sandbox just as we would do in dynamic analysis. We may then use our power over the sandbox to subject the adversary to various conditions and observe its behaviour. As a consequence, the first goal of such a cryptographic security proof is to show that we can simulate the "world" that our malware-née-adversary expects. Just like malware our adversary could decide to behave differently when it detects a simulation to avoid being analysed. In our setting the adversary expects two things – a Random Oracle and a decryption oracle – and we better simulate those (nearly) perfectly.

In this view, the ROM is Hashing-as-a-Service (HaaS). Instead of specifying a compact hash function like SHA2 with all details so that anyone can ship their own implementation, we are just going to define some API with a single calling point H(): put some string in, receive a digest back, e.g. y=H(x). In the ROM, our HaaS also realises a perfect hash function: for each fresh input x it returns a completely random digest y (of course, if we call H() again on the same x we get the same y just as we would expect from a hash function), so the only way to know the output y is to call H(x) via our API. So what we have is something "random" (perfectly random output) from an "oracle" (we can only call the API). This is somewhat similar in spirit to ransomware countermeasures that intercept calls to the cryptographic API provided by the OS. The difference is that ransomware may implement and ship its own cryptography, but in our thought experiment the only way to get access to H() is via our API. Another practical analogy would be HMAC with a secret key running on an HSM, something Facebook is using for password hashing.

Returning to our proof sketch, we want to show that the ability to decrypt every ciphertext except C does not buy the adversary anything. We can accomplish this in the ROM by making our construction dependent on our API s.t. the only way to produce a valid ciphertext is to call H() on the message (and any other randomness used during encryption), everything else produces an error on decryption. When we accomplish this (which isn't too hard) then the adversary has two choices: it can submit whatever it wants for decryption which will just produce an error or it can dutifully call H() via our API when producing a ciphertext. The key observation now is that in the latter case it sends us the message (and associated randomness) it might ask us to decrypt later. So we can easily provide plaintexts in response to correctly formed ciphertexts: we are cheating and know the answers before seeing the question.

From this we can conclude that if there was an adversary against our scheme that requires a decryption oracle we can run this adversary against our scheme without actually having access to such a decryption oracle (by simulating it using the information the adversary helpfully sends us via calls to H()). This implies that CCA attacks, i.e. active attacks – in the ROM and for schemes where such proofs exists –, are no more powerful than CPA attacks, i.e. passive attacks. To drive home this point, this is not a claim that we prevent the adversary from running specific attack strategies but it rules out any attack using such a decryption oracle. If we can fake it, it offers no advantage.

HaaS/the ROM is an incredibly powerful tool for proving security. Once we have HaaS we can play all kinds of tricks with the adversary. For example, we can start cheating and send specifically chosen answers in response to strategically chosen queries. When H() is used to check the integrity of some input x against some known digest y we can simply make our API return y on input x or z, it is up to us. This is known as "programming the Random Oracle". An analogy from dynamic analysis could be to provide bad randomness to a piece of malware to break its encryption or to return incorrect time/date information from a system call to trigger some behaviour. Another trick we can play is to restart our VM from a snapshot which is known as "rewinding". For example, we may choose to rewind the sandbox with the adversary to some point in the past and then provide different responses from our random oracle to provoke a fork in the malware: it started out doing the same but then at some point it performs different steps. The lemma proving that this makes sense in cryptographic security proofs is aptly called the "forking lemma".

The ROM isn't without its problems. For starters, HaaS isn't how we use hash functions, we actually implement them in code. Indeed, there are (arguably contrived) counter examples of cryptographic schemes that can be proven secure in the ROM but are insecure when used with any real hash function. Secondly, when we worry about quantum computers we also need to worry about hash functions being implemented on them. To account for this we would need to define quantum Hashing-as-a-Service where the adversary can send superposition queries and receive a superposition of digests back. In such a setting, the "looking up the plaintext for a ciphertext from previous hash queries" trick doesn't work any longer. Reproving cryptographic schemes in the Quantum Random Oracle Model (QROM) is an ongoing research endeavour.

Fortified Petrol Station in Calais

# THREE WEEKS IN CALAIS

Laura Schack

> PhD student Department of Politics, International Relations and Philosophy and ISG

Last year I spent three months in France, Greece and Italy conducting field research. I began in May with three weeks of participant observation research volunteering in Calais. Alongside conducting dozens of research interviews, I chopped vegetables in the Refugee Community Kitchen, sorted clothes donations in the Help Refugees warehouse and regularly went out on distributions to bring food and clothes to the hundreds of refugees living rough in the area in informal settlements.

Calais' security infrastructure, funded by both the UK and the French governments, was part of daily life there: the CRS, the French riot police, were everywhere in their distinctive vans, watching the volunteers on their distributions; many asylum-seekers I met would talk about the regular, and often brutal, evictions of their settlements by the police; and fences, walls and barbed wire were permanent fixtures defining the landscape of Calais.

This clash between security structures and humanitarian spaces was evident throughout my three months in the field. I was conducting research for my PhD thesis on the criminalisation of pro-migrant civil society groups, including NGOs, activists and volunteers. This involved exploring the different ways in which state actors attempt to impede civil society efforts to aid migrants and asylum seekers throughout Europe – and the role of the digital both in facilitating and challenging this criminalisation.

Tensions between civil society actors helping migrants and state authorities have increased in recent years. The 2019 arrest of Carola Rackete [1], the Sea Watch captain accused of participating in migrant smuggling in Italy, is perhaps the most famous example. Others include the 2018 prosecution of the Stansted 15 activists [2] in the UK under terror-related charges, the tensions over refugee camps in Calais [3] and the 2018 arrest and detention [4] of Sarah Mardini and Sean Binder, two volunteers on Lesvos island in Greece who are still facing smuggling charges today.

## Competing logics of security

All this is taking place within the context of a highly securitised migration field, in which migration and the refugee crisis are seen as issues of security. For example, the European Commission's department of Migration and Home Affairs focuses on migration, security, and securing EU borders, and similarly, the UK Home Office is responsible for immigration, security, and law and order. The treatment of migrants and refugees as security threats has far-reaching consequences, including the ability of states like Turkey to use migrants as weapons [5]_with which to attempt to force Europe's hand.

I am supervised by both an academic from the Department of Politics and International Relations and from the ISG. This has meant bringing a security perspective to my work. I have found Roxanne Doty's (1998) three modes of security particularly useful as a framework for analysing the security structures I encounter in the field. My research is primarily situated within the tension between two of these security modes: logic of national security and logic of human security.

The state response to the refugee crisis, as represented in the walls, barbed wire and the police presence in Calais, has been one following the logic of national security. The national security logic emphasises the distinction between insiders and outsiders, between "us" and "them", and is closely tied to territory. As this is the classic security logic of wars between nation states, it also results in militarised responses – in walls, weapons and force. These responses not only result in humanitarian disaster and the loss of life at and within Europe's borders, but they are also ineffective and fail to prevent irregular migration.

The civil society response to the refugee crisis, which has seen thousands of people around Europe volunteering their time and money to help migrants and refugees, follows the logic of human security. Human security is inclusive and pluralistic, it recognises the right of individuals to security over the more abstract concepts of security for territories, nations or societies. By fighting to ensure security for individuals, civil society groups, such as those providing food and clothing to homeless refugees in Calais, are in direct opposition to the national security logics practiced by states. And by attempting to include those that states would wish to exclude, civil society groups have found themselves in the line of fire.

### The digital battleground

//////////////////////////////////////////////////////

Whilst Doty's thinking might not immediately seem like a natural fit for work within the ISG, this conflict, in fact, is playing out in the digital sphere as much as in the physical and Doty's three modes of security offer insight into how digital security is used and the security it offers for whom. Civil society groups organise, communicate and gain support on online platforms while physical state border infrastructure is becoming increasingly integrated with the digital. And as riot police in Calais intimidate volunteers with their physical presence, state actors also target civil society groups through digital means. The Iuventa, the search and rescue ship of a German NGO, was bugged by the Italian authorities prior to its confiscation [6]; Loan Torondel, a volunteer in Calais, was fined on criminal defamation charges for a tweet he had published accusing police of taking away a refugees' blanket [7]; and WhatsApp messages constitute key evidence in the cases against 35 volunteers being investigated on smuggling-related charges alongside Binder and Mardini in Greece [8].

But the digital is also a space in which civil society groups are able to fight back against the authorities targeting them. For example, search and rescue boats conducting rescue operations in the Mediterranean now ensure that they create meticulous digital records of their activities which can act as evidence in court. And civil society groups around Europe act as witnesses and document and publicise human rights violations by state actors, including the brutal police evictions [9] in Calais, and are thereby able to draw media attention and hold states to account. When I ask my interviewees whether they worry their devices or accounts are being bugged or hacked by police, they often reply 'yes, but I don't care. I'm not doing anything wrong. They are.'

My studies indicate that digital stand-offs such as the ones I came across often exacerbate tensions. However, applying social and political theories of security to digital practice offers new ways of understanding and potentially responding to such conflict. As the digital becomes a place where individuals meet the state with increasing frequency, the more we learn about the different ways in which these interactions play out, and the ways that digital technologies shape the nature of these interactions, the better we will be able to present security strategies that are less adversarial and more mindful of the constructive roles that digital technology can play in conflict resolution.

[1] https://www.bbc.co.uk/news/world-europe-48853050
[2] https://www.theguardian.com/world/2018/dec/16/migrants-deportation-stansted-actvists
[3] https://helprefugees.org/wp-content/uploads/2018/08/Police-Harrassment-of-Volunteers-in-Calais-1.pdf
[4] https://www.theguardian.com/world/2018/dec/05/syrian-aid-worker-sarah-mardini-refugees-freed-greece
[5] https://www.nytimes.com/2020/02/28/world/europe/turkey-refugees-Geece-erdogan.html
[6] https://www.zeit.de/gesellschaft/zeitgeschehen/2019-05/saving-refugees-mediterranean-luventa-matteo-salvini/komplettansicht
[7] https://www.hrw.org/news/2019/06/25/france-aid-workers-defamation-conviction-upheld
[8] https://www.hrw.org/news/2018/11/05/greece-rescuers-sea-face-baseless-accusations
[9] https://helprefugees.org/wp-content/uploads/2019/06/Forced-Evictions-in-Calais-and-Grande-Synthe-ENG-1.pdf

# WISDOM 2019-2020 ROUND-UP

Rachel Player
Elizabeth Quaglia

> Lecturer ISG
> Senior Lecturer ISG

It's hard to believe that it has been four years since the WISDOM group was founded in 2016 by former PhD students Dr Sheila Cobourne and Dr Thyla van der Merwe. WISDOM (Women In the Security Domain and/Or Mathematics) was born out of the recognised need to increase diversity in the fields of Mathematics and Information Security, and to support the women already working in these fields. In 2017, WISDOM was honoured for its efforts with the Enhancing Fairness Award in the annual Principal's award ceremony at Royal Holloway, and since then the group continues to go from strength to strength.

WISDOM's efforts are coordinated by a committee of mathematics and ISG PhD and MSc students, currently led by co-presidents Lydia Garms and Catherine Keele. The 10-strong committee includes representatives responsible for the organisation of events, outreach efforts, and socials. The mailing list counts over 100 members, who are invited to attend events and volunteer in outreach efforts (new WISDOM members are always welcome!). The most recent WISDOM social saw around 25 participants.

In the early days, the WISDOM group worked hard to establish itself as a network to support and raise the profile of women working in Information Security and Mathematics at Royal Holloway. This was achieved by hosting now-traditional events such as the MSc networking lunch at the start of the academic year, and the Winter Networking Event at the end of the first term. WISDOM also hosted a local edition of the Voice & Influence Program [1], an online curriculum designed to empower women and men to realise their professional potential and help them create organisations where workers can excel and thrive.

At that time, the WISDOM group also set out a vision, including the goals to support and receive support from other internal and external groups with similar objectives, and to encourage more women to study mathematics and information security. It is in these two areas that WISDOM has made significant progress in 2019-2020, by expanding its network further and extending outreach efforts. Several activities and initiatives have been organised by the very proactive committee, and attendees included staff as well as students at the PhD level right through to undergraduate. In this article we share details of those activities, and tell you how to get in touch if you'd like to get involved in the future.

We kicked off in October with the annual MSc welcome lunch, and an event to mark Ada Lovelace Day, an international celebration of the achievements of women in STEM. Both events were very well attended and provided the opportunity to welcome new students to the department. To celebrate Ada Lovelace Day, WISDOM teamed up with Women in Biology to put on an event featuring discussions, a 'gender equality' quiz and refreshments. The LGBT+ Staff Network and RoWaN (Royal Holloway Women's Network) were also invited, to create links with other diversity networks in the college. This also allowed new students the opportunity to learn about the different support groups that are available to them.

November half term saw a group of PhD student volunteers coordinated by the WISDOM outreach officers leading an outreach activity at the Science Museum. This was part of the Top Secret exhibition [2], which took visitors on a tour of codebreaking and cyber security from the First World War up to the present day. WISDOM engaged visitors in a hands-on magic trick about binary numbers.

In December, WISDOM members enjoyed an informal social over pizza and watched Hidden Figures, the 2016 film based on the lives of black women working for NASA in the 60s. Also in December, the annual Winter Networking event took place. Guest speakers Anne Benischek and Rachel Player spoke about their experiences working in cyber security as a woman in industry and academia respectively.

In January, WISDOM launched the Tampon Initiative, providing free sanitary products in dedicated boxes found in Bedford Building restrooms. The initiative was inaugurated with an invited talk by CDT student Laura Shipp on period poverty. February saw another first for WISDOM, as members took a break from their desks to participate in a seated yoga session.

In March, WISDOM celebrated International Women's Day with a pub quiz social. Four teams battled it out to answer questions on the theme of International Women's Day. The quiz writers took the opportunity to feature many more women in the answers than in a typical pub quiz. For example, in a music round about duets, the male singer was given, and the participants had to name the female singer. To emphasise the international component, the writers also tried to make the questions less UK-centric than is typical. One of the quiz writers, WISDOM committee member Erin Hales, commented: "it was great to see everyone getting involved and being able to contribute answers. The pub quiz regulars didn't have much of an advantage and the scores ended up being very close!"

If you'd like to know more about WISDOM, follow us on social media where we share all the details of our upcoming events: we're active on Facebook, Twitter and LinkedIn. WISDOM also maintains a blog where contributors share their thoughts and personal experiences on topics such as diversity and inclusion. We welcome guest contributions, so please get in touch via wisdom@rhul.ac.uk if you have something to share.

[1] https://womensleadership.stanford.edu/voice
[2] https://www.sciencemuseum.org.uk/what-was-on/top-secret

Left: WISDOM launched the Tampon Initiative

# ON THE OCCASION OF PROFESSOR FRED PIPER'S RE-RETIREMENT

Robert Carolina

> Senior Visiting Fellow ISG

----

***HP/HPE Colloquium Day Royal Holloway University of London***

----

**19 December 2019**

----

Good afternoon, ladies and gentlemen.

Many of you know me. My name is Rob Carolina and I'm with the Information Security Group here at Royal Holloway. I've been asked to say a few words about a change that's happening here. Many of you know that Professor Fred Piper – theoretically – retired from the ISG more than 15 years ago. But we all know that there is a stark difference between theory and reality. From the moment his retirement party ended, Fred has continued to serve the university and the ISG as a consultant. He has generously dedicated enormous time and energy to assist and support the ISG and its many members.

I'm sorry to announce that Professor Piper has advised the university that he does not wish to continue that consultancy beyond the end of this calendar year. In other words, Fred has decided to upgrade his theoretical retirement to actual retirement.

Since this will be Fred's last appearance at this Colloquium in an official capacity, I've been asked by my ISG colleagues to say just a few words to mark the occasion and they have kindly suggested a few observations.

Fred has been a pioneer and a visionary. Fred developed the first cryptography research group in the history of UK higher education. The book on Cipher Systems that he co-authored with Henry Beker was published in 1982, became an industry reference and stood virtually alone in what was then a new field.

He helped to create the first masters degree in information security, the first UK academic group focussed on information security, and the first distance learning programme in information security. But this is more than a story of academic achievement.

Part of Fred's magic – and the success of the ISG – came from his tireless efforts to engage with industry and government. As he said to me recently,

> "We succeeded because we asked what people in industry wanted, and we listened to what they told us. We didn't always do what everyone wanted, but we listened and we did a lot of it."

In an age when people speak of "impact", any visit to Fred's office clearly demonstrates part of his legacy and contribution to the field – volume after volume of completed PhD dissertations that he supervised over the course of decades, including the work of a very young Michael Walker whose PhD was awarded in 1973 and whose contribution to mobile security will feature so prominently in today's final session.

Amazingly for someone who is so intricately bound up with the founding, growth, and success of the ISG, Fred somehow managed to accomplish these things while also trying very hard to stay out of the limelight. That's how I know he's so very uncomfortable now, and why I have to finish this quickly.

I've only known Fred for 25 years. And in that time, Fred has consistently gone out of his way to describe the accomplishments of other people in the ISG. How the success of the ISG was a group effort. How the growth of the ISG was based on creating a community of interest both inside and outside of academia. How the field of information security has advanced through the efforts of many.

And yet, a common theme echoed by my colleagues is this: we would not be here today, this university would not have an information security group, we would not have a legacy of thousands of masters degree graduates and hundreds of PhD graduates, if it weren't for Fred.

So now I ask all of you to please join me in showing our appreciation to someone who does not seek praise, but who certainly deserves it.

**THANK YOU FRED!**

Participants of Homomorphic Encryption Workshop 2020. Microsoft Research, Redmond, USA. 6 February 2020.

# HOMOMORPHIC ENCRYPTION STANDARDISATION

Rachel Player

> Lecturer ISG

Fully homomorphic encryption enables the evaluation of arbitrary functions on encrypted data. This technology can enable many applications which may otherwise not be possible, in diverse areas such as genomics, healthcare, critical infrastructure and finance. Alongside other Privacy Enhancing Technologies (PETs), homomorphic encryption is emerging as a crucial tool for privacy-preserving data analysis.

A homomorphic encryption scheme comprises the usual key generation, encryption and decryption algorithms, as well as an evaluation algorithm, which provides the additional functionality. Suppose a client owns data x and wishes to outsource the computation of a function F(x) on the data to a cloud server. The client sends an encryption of their data x, and the function F, to the server. The server then runs the evaluation algorithm, which takes as input the encrypted data and F, and outputs an encryption of F(x). The “magic” is that the server does not need to access the secret key in order to perform this evaluation. Moreover, the server does not learn F(x), only an encryption of it, which is sent back to the client. Only the client, holding the secret key, is able to decrypt and obtain the result F(x).

Achieving fully homomorphic encryption was proposed as an open problem by Rivest, Adleman, Dertouzos in 1978, and was not resolved until Gentry’s 2009 thesis. Gentry’s proposal and other early schemes were huge theoretical advancements, but far from practical: processing on ciphertexts was 10 to 12 orders of magnitude slower than the same computation on plaintexts. In addition, there was relatively little in the literature around concrete applications of homomorphic encryption before 2011. This has contributed to an unfortunate and persistent reputation of homomorphic encryption being totally impractical.

This is no longer the case, and more recent schemes and implementations have made great progress towards improving performance, for example by developing techniques to better encode raw data into plaintexts. In fact, we are now almost at the point of commercial viability for certain applications, with interest from large tech companies as well as several start-ups. Alongside this, an effort to standardise homomorphic encryption was initiated in 2017 by HomomorphicEncryption.org, an open consortium of participants representing industry, government and academia. Researchers from the ISG have been involved throughout this process and have contributed to the Security Standard [1] published by the consortium in late 2018.

The hard problem underpinning the security of homomorphic encryption schemes that are widely used today is the Learning with Errors (LWE) problem. Informally, this problem asks to recover a secret vector s given a pair (A, b), where the matrix A is chosen uniformly at random and the vector b is formed by taking the product of A and s and adding an error vector e. The Security Standard recommends several LWE parameter sets that implementors can select from in order to achieve a certain target security level.

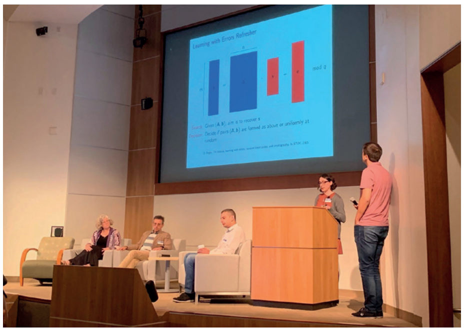
CDT student Benjamin R. Curtis and I led a discussion at the most recent standardisation meeting in August 2019 on possible extensions to these LWE parameter sets. We investigated a number of possible improvements and published [2] our results at the 7th Workshop on Encrypted Computing & Applied Homomorphic Cryptography which was associated with CCS 2019. In February 2020 Benjamin and I participated in a workshop hosted at Microsoft Research, Redmond, where we set to work on making the agreed updates to the Security Standard.

The main goal of the February 2020 workshop was to articulate community priorities for homomorphic encryption standardisation in the next 2-3 years. I had the opportunity to share my thoughts in a lightning talk, and apart from updating the Security Standard, a key goal for me is around usability. At present, it is fair to say that one has to be an expert in homomorphic encryption in order to be able to implement applications built from it in a performant way. On the other hand, the likely developers using homomorphic encryption libraries may not be trained in cryptography but rather in machine learning or bioinformatics. This needs to be reconciled, and an important direction would be to develop automatic parameter selection tools that can help users identify parameters that balance performance, correctness and security.

References:

[1] Martin Albrecht, et al. Homomorphic Encryption Security Standard. HomomorphicEncryption.org, Toronto, Canada. Nov 2018. Available at: https://eprint.iacr.org/2019/939.pdf

[2] Benjamin R. Curtis and Rachel Player. On the feasibility and impact of standardising sparse-secret LWE parameter sets for homomorphic encryption. 7th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, WAHC@ CCS 2019, pp 1—10, 2019.



CDT student Benjamin R. Curtis and I lead the security standard panel discussion at the 4th HomomorphicEncryption. org standards meeting. Intel AI, Santa Clara, USA. 17 August 2019. Also pictured (L – R): Kristin Lauter (Microsoft), Daniele Micciancio (UCSD), Yuriy Polyakov (Duality).

# RESOURCE ESTIMATION GONE QUANTUM

Eamonn Postlethwaite
Fernando Virdia

**> ISG PhD Students**

The past ten years have seen promising developments in the field of quantum hardware engineering. In this area, the Grail would be a general purpose, error tolerant, quantum computer. These developments have not gone unnoticed by state entities and standardisation bodies. Such a quantum computer could execute more powerful cryptanalytic attacks on current encryption schemes, putting secure communications at risk everywhere. For this reason, there are ongoing international efforts to design cryptographic solutions that are not affected by quantum computers [1].

Cryptographic security assessments consist of developing attack strategies against a cryptographic primitive, and then estimating how many resources (e.g. time, electronics, energy, communication, money) would be required to execute them. We generically refer to these as the cost. Quantum resource estimation consists of calculating the cost for attacks that require a quantum computer.

In this article we will look at two of our recent papers regarding two different aspects of resource estimation for Grover's quantum search algorithm. Grover's is a landmark achievement in quantum computing. It can play a role in many quantum cryptanalyses as it finds, in approximately $\sqrt{n}$ steps, an arbitrary element in a list of length n that has been randomly shuffled. Its theoretical advantage over classical search, which would require about n steps, provides a great foundation to analyse the possible practical disadvantages and complications of quantum computation.

A popular tool for designing quantum safe cryptographic schemes are lattices. These are objects formed of infinitely many points in a space. To break these schemes the most effective algorithms seem to be lattice sieves. These search a large list of lattice points, say of size n, in a clever way, looking for points that are close in space. The larger the dimension of the space, the bigger this list, this n, is. As a search problem, lattice sieving is a prime candidate for Grover's algorithm.

The result of using Grover's in lattice sieves is a quantum algorithm that requires significantly fewer steps than its classical counterpart. Yet, comparing the concrete difference in required resources between classical and quantum lattice sieves is hard. Classical steps and quantum steps are different operations, that run on fundamentally different hardware. Hence, it is not immediately clear that fewer (that is, $\sqrt{n}$) steps of quantum search result in smaller costs than n steps of classical search. One could speculate that, in practice, for low dimensional lattices, quantum sieves may not provide a lower cost.

In classical circuits, quantities are represented as bits, which can take a value of 0 or 1. Modern electronics are good at maintaining bits in their correct state. The situation differs for quantum circuits. Quantum algorithms use more detailed quantities, in the form of qubits. Unlike in the classical case, it is not known how to build quantum circuits where the values of these qubits remain stable. To protect the circuit from errors being introduced, each qubit must be repeatedly measured, error corrected, and reinitialised. These are all classical operations! If we can talk about the cost of a quantum step in terms of the classical cost of this error correction, then we can compare part of the cost of quantum sieving to that of classical sieving.

In recent work [2], we design efficient quantum circuits for a component shared between many performant lattice sieves and then describe quantum cost metrics that capture the cost of error correction. We use these to determine the practical overhead of running Grover's algorithm. If the dimension of the lattice is high enough, then the overhead will still be less than the efficiency gained from only requiring $\sqrt{n}$ steps, and quantum sieves will beat classical sieves. Yet, for lattices relevant to cryptography, we find that the cost of error correction alone is close to the overall cost of classical sieving, and hence may justify not considering quantum sieving during cryptanalysis.

Another application of Grover's is exhaustive key search. The idea of this attack is that, even if there is no weakness in your encryption algorithm, one can still guess the correct decryption key by trying every possible one. NIST, the standards body running the main quantum-resistant cryptography effort, asked the proposers of candidate solutions to argue why breaking their scheme is as hard as running key search against the AES block cipher suite.

On classical hardware, key search against AES-128 (from now on AES) requires about 2^128 steps, each an independent execution of the AES circuit lasting a (small) unit of time. This could mean an attack taking 2^128 (units of) time, using a single machine, but also an attack taking 2^96 time using 2^32 machines in parallel. We can think of the total cost of the attack as the cost to run each machine for the duration of the attack times how many we run. Both attacks above have the same total cost, because 32 + 96 = 128, even though the second strategy takes less time. We say classical exhaustive search is embarrassingly parallelisable. This property allows us to talk of "2^128" cost, even if no adversary will ever attempt to sequentially run 2^128 instances of AES on the same machine.

Grover's algorithm is not embarrassingly parallelisable. To cut execution time in half, one needs four times the number of machines. For example, if key search on a single quantum computer would take 2^64 quantum steps due to the Grover's speedup, using 2^32 quantum computers would bring the number of sequential steps down to 2^48. Since 32 + 48 > 64, the total cost increases after parallelisation. This tradeoff means that running the quantum attack within a fixed amount of time (by using parallelisation), will have a different total cost than running it without time constraints.

In a recent paper, [3] we look at key search within the time constraints for quantum attacks proposed by NIST. We investigate possible parallel-friendly designs for AES quantum circuits and optimise parallelisation strategies. We show both that AES may be easier to attack with a quantum computer than estimated by NIST, but also that it will still be much harder than what quantum algorithm theory suggests at first glance.

We would like to conclude by pointing out that the two approaches to quantum resource estimation could and should also be considered simultaneously; applying time constraints to sieving and measuring error correction costs for key search. We would also like to suggest that, given the apparent complexity of building an error-tolerant quantum computer, and the issues in parallelising some quantum algorithms such as Grover's, it could be useful to rethink the way we design quantum algorithms, by targeting Noisy Intermediate-Scale Quantum (NISQ) computers instead [4].

[1] See Martin R. Albrecht's article in the 2018-19 ISG newsletter.

[2] Albrecht, Gheorghiu, Postlethwaite, Schanck, "Quantum speedups for lattice sieves are tenuous at best", https://ia.cr/2019/1161

[3] Jaques, Naehrig, Roetteler, Virdia, "Implementing Grover oracles for quantum key search on AES and Low MC", https://ia.cr/2019/1146.

[4] Preskill, “Quantum Computing in the NISQ era and beyond”, https://arxiv.org/abs/1801.00862.

Above & Above Right: pictures from the main conference and registration desk at CCS 2019

# UPDATES ON THE SYSTEMS & SOFTWARE SECURITY LAB (S3LAB) - 2020

JORGE BLASCO ALIS, JASSIM HAPPA, DAN O'KEEFFE, DANIELE SGANDURRA

Systems & Software Security Lab

BLEMAP

The Systems & Software Security Lab (S3Lab) was established in September 2018. S3Lab's main research focus is analysing the security of software, namely how it is being designed, developed, deployed and used from the processor level up to the application layer, by addressing three main areas: smart-devices, desktop, and Cloud. We investigate how software vulnerabilities are introduced and exploited, and design novel mitigation techniques to address them. We also advocate a more proactive approach, e.g. by designing and testing evasive techniques against existing software protection mechanism – the goal being to provide more robust mitigation solutions. Our methods range from the use of machine learning to techniques such as data-flow analysis to control-flow integrity and recent developments in trustworthy computing.

S3Lab includes 18 people: staff members, PhD students and research assistants. The past year has been a highly productive period for S3lab as we have been involved in several activities, some of which are described in this article. Please visit our website (available at: https://s3lab.isg.rhul.ac.uk/) to find out more about our ongoing activities and projects.

## Ongoing projects: focus on BLEMAP

//////////////////////////////////////////////////////////

The S3Lab was part of the third cohort of the Cyber Academic Start-Up Accelerator (CyberASAP) with BLEMAP. BLEMAP is the result of S3Lab's research efforts in Bluetooth security. BLEMAP gives insight into what Bluetooth devices do and how secure they are. The technology, developed thanks to the CyberASAP program funded by DCMS, identifies security threats in a wide range of Bluetooth devices, enabling organisations to secure their wireless environments. The funding provided by DCMS has allowed the S3Lab to take BLEMAP to a minimum viable product stage.

## Highlights of events and research activities

//////////////////////////////////////////////////////////

CCS 2019 – experience with registration. Members of the S3Lab organised the registration for the 26th ACM Conference on Computer and Communications Security (CCS), which was held in London, from 11 to 15 November 2019. The conference, with more than one thousand attendees, is one of the top academic conferences in Information Security.

CYSARM @ CCS 2019. A member of the S3Lab organised and chaired the 1st Workshop on Cyber-Security Arms Race (CYSARM), held on 15 November 2019 as part of CCS. The CYSARM'19 call for papers attracted submissions from 13 countries, from a wide variety of academic and corporate institutions. In total, CYSARM received 21 valid submissions, of which 4 papers were selected as Full Papers and 1 paper was accepted as a Short Paper. The 2nd edition of CYSARM will be held in Orlando, USA, on 13 November 2020, co-located with CCS 2020. The CYSARM'20 call for papers can be found at the website: https://www.cysarm.org/.

C2C-CTF 2020. Members of the ISG and S3Lab will organise the 1st edition of the Country-to-Country (C2C) Capture the Flag (CTF) competition, which will be hosted at Royal Holloway, in Winter 2020 (to be confirmed). C2C-CTF 2020 is the start of a five-year academic plan to host cyber-security competitions in five different countries led by International Cyber Security – Center of Excellence (INC S-CoE). C2C will extend past experiences and lessons learnt from the successful Cambridge2Cambridge CTF, with its global vision to entice thousands of people worldwide to study cyber security at university-level. C2C will be an exciting opportunity for students to work together as international teams to solve interesting CTF challenges, while learning new skills, socialising, and promoting international collaboration and friendship. Please stay tuned to the C2C-CTF website for more information: https://www.c2c-ctf.org/

Paper accepted at 16th ACSAC Conference 2019. The paper titled "A Game of “Cut and Mouse”: Bypassing Antivirus by Simulating User Inputs" has been accepted and presented at the 35th Annual Computer Security Applications Conference (ACSAC 2019). The paper is co-authored by Daniele Sgandurra, in collaboration with Ziya Alper Genç and Gabriele Lenzini, from the Interdisciplinary Centre for Security Reliability and Trust (SnT).

Papers accepted on “Alternative Threat Detection”. Jassim Happa has recently co-authored two papers on alternative threat detection methods. The first one: "Sonification to Support the Monitoring Tasks of Security Operations Centres" (IEEE Transactions on Dependable and Secure Computing) examines how threat detection analysts can make use of both audio and data visualizations of network traffic patterns as a way to investigate attacks. This was a collaboration with Louise Axon, Alastair Janse van Rensburg, Michael Goldsmith and Sadie Creese from the University of Oxford. The second one: "Anomaly Detection Using Pattern-of-Life Visual Metaphors" (IEEE Access) explores the feasibility of using visualizations to make people become anomaly detectors with city landscapes and galaxy clusters visualizations created from host-based activities. This was a collaboration with Thomas Bashford-Rogers, Ioannis Agrafiotis, Michael Goldsmith and Sadie Creese from the University of Oxford.

Highlights of PhD students

//////////////////////////////////////////////////////////////

Voice Personal Assistant Security (Sergio Esposito) shares the following highlight: Devices like Amazon Echo and Google Home are gaining popularity at a steady pace. While the Internet of Things was already a reality many years ago, being able to control a Voice Personal Assistant (VPA) -- and possibly our entire home -- with the aid of our voice only is a recent novelty. This, of course, comes with several security problems and, although the security research field on VPAs is rather fresh, new attacks, problems (and solutions!) are being discovered and developed at a fast pace sometimes with remarkable results. For example, some papers show how to generate inaudible audio tracks that hide malicious commands for VPAs by means of psychoacoustics, ultrasounds, or even light. So far, the research has mostly focused on attacks that are possible when the VPA doesn't understand correctly the user's request, or on authenticating the user with their voice only, e.g. to block unauthorised users in issuing malicious commands. I'm really intrigued by the fact that so much has been discovered in such a short timeframe and that there is still a lot to discover. In these initial months of my PhD, I've already learnt a lot on the research field and on the research methodologies, and I'm looking forward to giving my contributions to better understand, and improve, the security of VPAs.

1ST WORKSHOP ON CYBER-SECURITY ARMS RACE (CYSARM)
November 15, 2019
Venue: Hilton London Metropole
225 Edgware Road, London, UK
co-located with the 26th ACM Conference on Computer and Communications Security

# ALL ROADS LEAD TO PEOPLE…

Helen L

> Technical Director for Sociotechnical Security, National Cyber Security Centre

[In this article Helen L sets out NCSC's programme to enable better cyber security through multidisciplinary research into people, technology and their interactions. The ISG has contributed to NCSC's sociotechnical security programme since its inception and is a founding member of the NCSC-supported Research Institute in Sociotechnical Security (RISCS). Lizzie Coles-Kemp is the current RISCS Fellow for Digital Responsibility.]

I have worked in Security for almost 20 years now and the last 10 years of those have been in Cyber Security. As a Physics graduate, I began my career at GCHQ researching the atomic level material properties of semiconductor substrates to better understand how they behave in different environments and contexts. My next post took me into the field of systems engineering. I was asked to establish a research portfolio (and a team) that would understand how cyber security could be woven into the fabric of a development process. This was to help answer questions like ‘how we can gain confidence that the product being built will be secure?’ and ‘how can we ensure that security is usable and will work as we expect it to in practice’? What emerged was that, despite the heavy contextual focus on hardware and software in those roles, often the solution resided in a sociotechnical space, not just the technical one. The consideration of people was a lens that everyone had frequently forgotten to look through.

The Sociotechnical Security Group (StSG) at the NCSC was set-up in 2016 to do just that: explore the relationship between people and technology. The things that, hitherto, had fallen down the cracks; that historically we had plastered over with a technological or policy solution. In the StSG we’re all about finding those cracks, understanding how they have come about, working on how we might prevent them from happening again in the future and reducing the harm that the existing ones might cause.

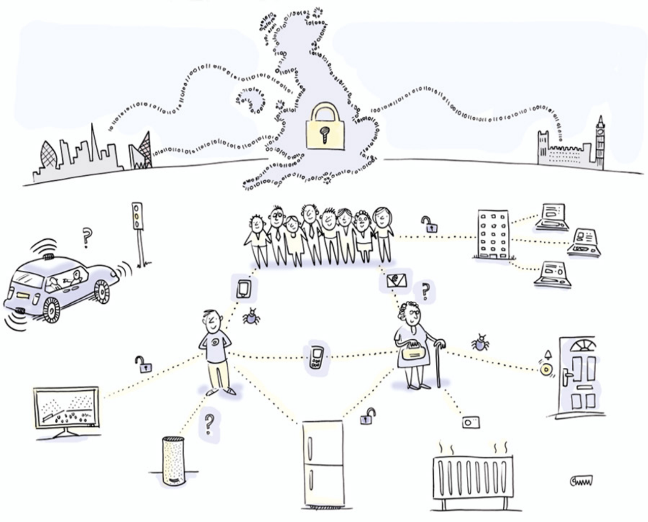
Our unique perspective and insights on cyber security support much of what we do and achieve in the NCSC to make the UK the safest place to work and do business online; and are testament to the importance and power of a multidisciplinary approach to cyber security.

## The jigsaw pieces

The epicentre of our research portfolio is all about understanding people: how they behave, both individually and collectively. Whether they are a member of staff, a board executive, a member of the public, a victim of cybercrime or a developer… we use well-established social science methods to find out about their daily routines and relationship with security. These approaches are crucial for us to be able to develop an evidence base upon which to pitch our interventions and advice and guidance: we need to ensure it gets to and works for real human beings in the real world. Our Individuals and Families top tips, Cyber Aware messaging (for individuals and small organisations) and You Shape Security advice (for organisations) are fabulous examples of this in action. I’m also looking forward to introducing a portfolio that supports software developers to build secure and usable products in the near future.

## The StSG Focuses on a People-Centred Approach to Security

But simply understanding people is not enough; we also need to understand the interactions between people and technology. This is where disciplines such as Human Computer Interaction come in – they help us to gather insights about how to make our systems more usable, accessible and resilient. This is an area destined for real change as we are riding the waves of the digital transformation that has been thrust upon us by COVID-19. The psychological and physical boundaries between a person and their technologies is becoming increasingly blurred and it is not hard to imagine a future where they become indistinguishable. How can society trust an AI that we rely on to implement security-enabling functions in the future? How do people interact with intelligent machines? How do people draw insights and make risk decisions using data-



driven technologies? Traditional infosec technology-based techniques like network segregation, patching, software verification techniques, tick box risk assessments and some encryption approaches will be increasingly challenging to implement successfully in the real (or virtual!) world without a rethink. Instead we need to embrace a paradigm shift that distributes trust, placing it with people and processes too, rather than solely with the technology and data.

*K££P0ut!!*

The last piece of our StSG jigsaw is a systemic approach. I often use our Password Guidance to illustrate this point. If you asked me what qualities a "strong" password should have, I would say: the longer the better, be different to your other passwords and ideally comprised of random characters. That's fine if you have a handful of passwords, but in the real world people juggle many passwords across their home and work lives. Expecting them to choose tens of unique "strong" passwords and remember them rapidly becomes cognitively impossible. The outcomes are coping strategies like easy-to-guess passwords, password reuse and post-it notes on monitors…a worse result for security than if a simpler set of rules were put in place. A more holistic approach leads us to password policies that allow things like the use of password managers, storing passwords in browsers, using password generation strategies like 'three random words' and allowing people to write down and store their handwritten passwords in a secure way. We then start to see a risk-based approach and better security outcomes that enable a business rather than hinder it.

This same 'systems thinking' approach can also help us to support people to reason about complex systems. Whether that's through simulation and modelling of highly connected networks that we would never be able to comprehend with our human cognitive abilities, understanding how the markets in which cyber security operates behave, delivering systemic analyses for risk management or using anticipation and prospection to develop stories and narratives about the future. A systems approach is the perspective that enables us to have real impact in practice.

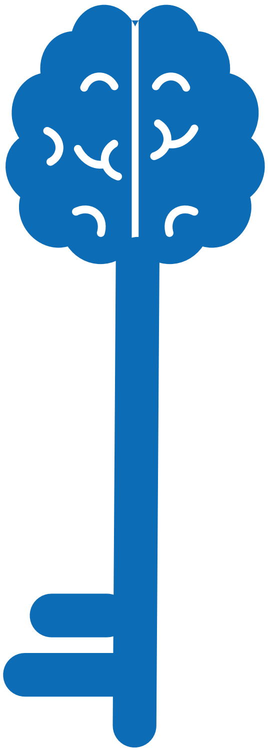
## Our "distributed brain"

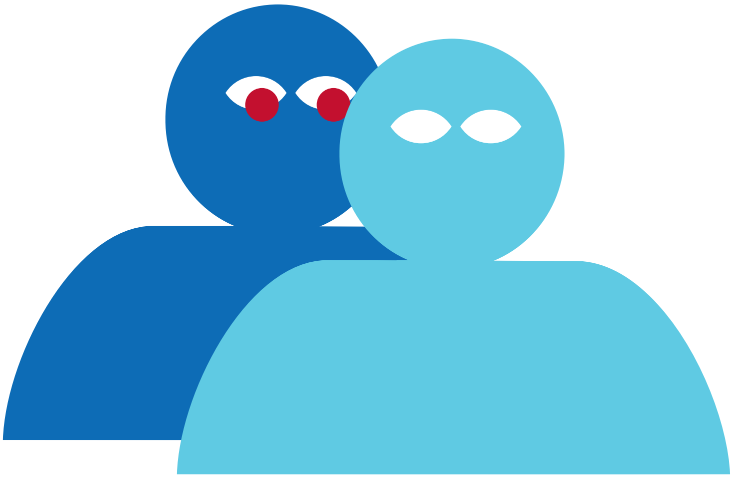
Of course, we cannot do this on our own. But to work effectively with others, we need to have more than snatched conversations on things in which we have a common interest. Instead, we need a shared vision that academia, government, industry and funding bodies can all buy into and contribute to. We also need a centre of gravity for this 'distributed brain' to ensure the whole is greater than the sum of its parts. This is what we're building through our Research Institute in Sociotechnical Cyber Security (RISCS), now in its eighth year.

This Research Institute, supported by NCSC, DCMS and EPSRC, has an open community spanning industry, academia and government. It brings together the best minds across many different disciplines: from anthropology to economics, mathematics to management science, engineering to classics and computer science to psychology. The magic happens when these diverse technical perspectives come together on a shared problem in a safe space to innovate.

We have identified five themes that we will focus on over the next year in RISCS: Leadership & Culture, Cybercrime, Secure Development Practices, Digital Responsibility and Anticipation & Prospection. As COVID-19 opens up many new technological opportunities and has accelerated us into a digital age where people and technology are increasingly intertwined and reliant on data, a multidisciplinary approach to cyber security becomes increasingly crucial. There are challenging and exciting times immediately ahead of us and I would like to invite you to consider how you and your research can contribute to the next stage of our sociotechnical cyber security journey.
This journey will be to the 'new normal', whatever that ends up being and it will be an inclusive journey, that works for real people in the real world.

I am eager to get going, I hope you are too. Please get in touch via either helen.l@ncsc.gov.uk or info@riscs.org.uk





# ALGORITHM SUBSTITUTION ATTACKS AGAINST RECEIVERS

Marcel Armour

**> PhD student ISG**

This article concerns some recent work undertaken by Bertram Poettering and myself, which looks at so-called 'Algorithm Substitution Attacks'. The starting point for this work w as the 2013 Edward Snowden revelations, in two senses:

1. In the sense that they inspired me to go down a path that led to me enrolling as a PhD student in information security; and

2. In a more important sense, they sparked a discussion by cryptographers, which our work engages with and builds on.

Our work is in conversation with two papers that have a strong link with the ISG. Following the Snowden revelations, Kenny Paterson together with Mihir Bellare and Phil Rogaway published 'Security of Symmetric Encryption against Mass Surveillance', which reinvigorated the study of subverted algorithms – whose heyday had been in the nineties under the name 'kleptography'. This work was followed up a year later, when Jean-Paul Degabriele, Pooya Farshim and Bertram Poettering (all ISG postdocs at the time) published 'A More Cautious Approach to Security Against Mass Surveillance'.

## Snowden Revelations

Thanks to the Snowden revelations, we know that mass surveillance is widespread and ongoing. Rather than breaking cryptography, the entities engaged in mass surveillance have used other avenues – adjacent to cryptography – to compromise the confidentiality and privacy of users. Examples include implanting malware, influencing public standards, accessing data and keys from corporations. This led the academic community to study subverted cryptographic algorithms.

## Subverted Algorithms

A subverted algorithm is one that has been replaced by (substituted with) the adversary's version, which will behave differently but in a way that is difficult to detect. Post-Snowden, it was Bellare, Paterson and Rogaway [1] who first showed how to design a subverted symmetric encryption algorithm. They also gave a formal model of an Algorithm Substitution Attack (ASA), defining such notions as the success and detectability of an ASA.

BPR's ASA against symmetric encryption worked by manipulating randomness to influence the choice of ciphertexts. Intuitively, when there are multiple possibilities for the encryption of a given message, observing that one is chosen over another leaks some information. If the information that ciphertexts leak is the user's secret key, then once the adversary has seen enough ciphertexts to recreate the whole key it can now decrypt all communication. As long as the ciphertexts from the subverted encryption scheme 'look like' real ciphertexts, then no one will be able to tell.

BPR also showed that subversion of symmetric encryption schemes can be thwarted by using deterministic (nonce-based) encryption as long as the encryption gives unique ciphertexts.

## Our Work

Degabriele, Farshim and Poettering [2] noticed that one of the assumptions made by BPR was very strict. BPR require that the sender's subverted ciphertexts all decrypt correctly according to the receiver's unsubverted decryption. But in practice, if one message in 2^128 (say) decrypts incorrectly this will never be spotted. In our work, we complement this approach. We keep the assumption of perfect correctness but interfere with the decryption algorithm.

We interfere with the decryption algorithm by subverting the authenticity guarantees that the decryption algorithm gives. Ciphertext authenticity can be achieved by using a so-called Authenticated Encryption (AEAD) scheme, and this is what we looked at in our work. AEAD schemes are widely used, and popular schemes include AES-GCM and OCB.

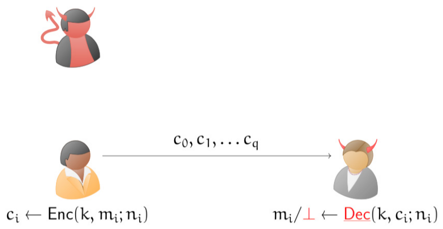
I will now give a high-level description of our attacks, as applied to AEAD schemes. This work was presented at IMACC in Oxford, organised by Martin Albrecht (ISG). After we completed this work, we realised that the attack can equally well be used to target Message Authentication (MAC) schemes.

## Our Attacks

We assume that the adversary can see whether a message decrypts correctly or not. There are practical scenarios where this is the case, for example if a decryption error results in a packet being dropped or retransmitted at a lower layer. Now when ciphertexts meet a certain condition, they are rejected despite being correct. The adversary can see this and knows that the rejected ciphertext meets the condition. From this, they can deduce something about the secret key.

Once enough ciphertexts have been (bogusly) rejected by the subverted receiver, the adversary has enough information to recover the key.

We also give a second attack which requires the adversary to intercept a valid ciphertext sent by the sender and tweak it to create a bogus ciphertext.


$c_0, c_1, \ldots c_q$
$c_i \leftarrow \mathsf{Enc}(k, m_i; n_i)$
$m_i/\perp \leftarrow \mathsf{Dec}(k, c_i; n_i)$

The adversary now sends the bogus ciphertext to the subverted receiver. If the bogus ciphertext meets some condition, it is accepted by the subverted receiver, who outputs the 'correct' message (corresponding to the original ciphertext). The fact that the bogus ciphertext has been accepted gives the adversary some information about the key. Once again, the adversary can use this to recover the key.

## Conclusion

Usually in cryptography, we assume that the algorithms used for encryption or decryption are honest and our notions of security are defined within this model.
The Snowden revelations tell us that the assumption that algorithms are honest does not necessarily hold, which led to the notion of Algorithm Substitution Attacks (ASAs). In our work, we contribute to the understanding of ASAs by proposing a new class of attacks that are undetectable according to previous models despite being highly practical by targeting the receiver rather than the sender. Thus, our work helps to refine the model as well as improving our understanding of what is possible for a mass surveillance adversary.

References:

[1] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of symmetric encryption against mass surveillance. In Juan A. Garay and Rosario Gennaro, editors, Advances in Cryptology – CRYPTO 2014, Part I, volume 8616 of Lecture Notes in Computer Science, pages 1–19. Springer, Heidelberg, August 2014.

[2] Jean Paul Degabriele, Pooya Farshim, and Bertram Poettering. A more cautious approach to security against mass surveillance. In Gregor Leander, editor, Fast Software Encryption – FSE 2015, volume 9054 of Lecture Notes in Computer Science, pages 579–598. Springer, Heidelberg, March 2015.

# ERROR-CORRECTING CODES: CRYPTOGRAPHY AND TELECOMMUNICATION

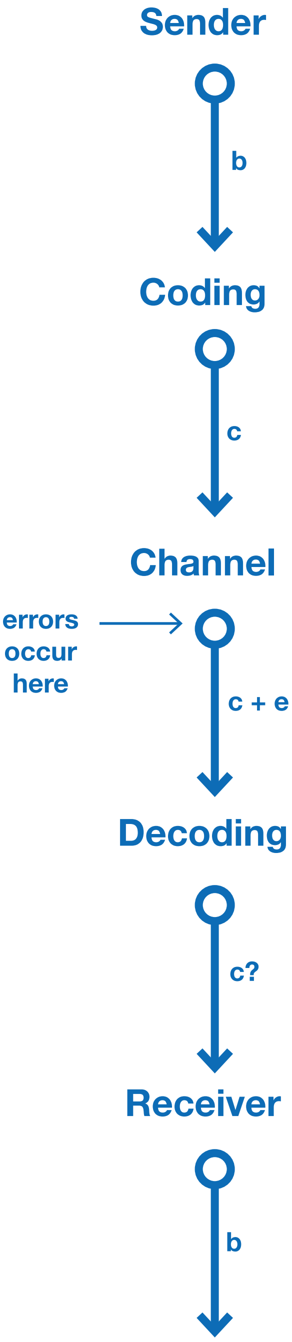
Thomas Debris

> Postdoc ISG

Post-quantum cryptography provides public-key cryptography resistant to adversaries with access to a large quantum computer. This kind of cryptography is based on problems coming from mathematical fields such as error-correcting codes or lattices. In this article, I will describe solutions based on error correcting codes.

Error-correcting Codes and Telecommunication. Let us forget about cryptography for a moment. The breakthrough of digital communication turned out to be feasible due to the availability of protection against ``errors''. Indeed, each bit of data that is stored or transmitted may be modified, either by the wear of time or due to a noisy channel of transmission. For those old enough, think about CDs, what happens if there are scratches? The principle enabling to recover data from a corrupted version of it is quite simple: redundancy. A banal example is when we want to spell our name by phone: A like Alex, L like Leo, B like Barbara… In a numerical context, we want to send bits, namely 0 or 1. The idea is the same as in the previous example. We add some redundancy. Suppose that we want to send a bit b to Bob who is on the other side of the Earth. If we only send the one bit b it might get flipped in transit (0 to 1 and 1 to 0). Instead of doing this, let us send this bit one hundred times. Therefore Bob gets a string of one hundred bits and he just decides that we sent zero if there are more zero bits or that we sent one if not. If there are less than 50 errors, Bob will recover the bit that we sent but if there more errors (too many scratches on the CD) Bob will make a mistake.

The procedure we just described is extremely onerous and slow, sending one hundred bits for transmitting only one bit. The goal of coding theory over the last seventy years has been to propose better mathematical structures of redundancy. This was done in order to send the lowest possible number of bits that still allow decoding to work even if there are many errors. The idea is as follows. Suppose that we want to send k bits b. Let C be a mathematical object which is called a linear code (it is just a subspace of GF(2)n of dimension k) with the following property. We can encode b into an element ofC , say, c. We added n-k bits to our string b to make a string of length n>k. Furthermore, we suppose to be able to recover b from c. The following picture shows a transmission scenario of b.



The operation which recovers c from c + e is called decoding. Decoding is a hard problem if we do not know any special structure onC and many mathematical structures onC have been proposed to solve this problem efficiently if the number of errors is not too large. For instance, 5G uses so-called ``Polar Codes''.

Error-correcting Codes and Cryptography. In his seminal work, McEliece proposed to use the decoding problem of a random code for public-key encryption. It is noteworthy that McEliece made this proposition in 1978, only a few months after RSA. The owner of the secret key, Alice, knows a codeC and some structure which enables her to solve the decoding problem for a number of errors. The public key simply consists in a ``scrambled'' version of the code, hiding the structure. To encrypt a message m, Bob encodes the message and adds a random error e. Decoding the message is assumed to be hard without knowing the inner structure of the code, but easy knowing it.

The challenge of code-based cryptography is thus to find codes which enable efficient decoding and whose structure can be hidden. From the theory of error-correcting codes we know many structures which enable decoding. This is good news for communication but we have to be careful in a cryptographic context. Many such structures are very rich and cannot be hidden. As a consequence, several of them were proposed in the last decades but subsequently broken. Nowadays we only know of a few structures that can be used in a cryptographic context: Goppa codes (McEliece's original proposal), MDPC codes or (U,U+V)-codes.

The proposal of (U,U+V)-codes is a relatively recent addition to the family of codes for cryptography and comes from the Wave signature scheme . It is a typical example of the approaches taken for making cryptographic codes: (U,U+V)-codes are a simplified version of Polar Codes which remove structure as much as possible. As a consequence, (U,U+V)-codes are significantly less efficient than Polar Codes and it would be stupid to use them in communication. However, they are of interest to cryptography since they still enable an efficient decoding algorithm and their structure can be hidden.

One of the major issues of code-based cryptography is to find codes like these with poor structure but with a decoding algorithm. Such codes will enable us to construct new cryptographic primitives.

Facebook:
Information Security Group (ISG) RHUL Official
facebook.com/ISGofficial

Twitter:
twitter.com/isgnews
@ISGnews

LinkedIn:
linkedin.com/groups?gid=3859497

You Tube
youtube.com/isgofficial

## CONTACT INFORMATION:

For further information about the Information Security Group, please contact:

Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX
United Kingdom

T: +44 (0)1784 276769
E: isg@royalholloway.ac.uk
W: www.royalholloway.ac.uk/isg