INTRODUCTION

The 2011-12 academic year saw dramatic expansion in Cryptography and Security research at the University of Bristol. The research group approximately doubled in size; page 2 onwards lists details of our new staff and PhD students. We were also awarded the status of Academic Centre of Excellence in Cyber Security as part of a new EPSRC/GCHQ initiative. Both applied and theoretical themes were well-represented in our research output, which continues to combine the two in a manner unique to Bristol.

The highlight of the year, though, was the hosting of Eurocrypt 2012 in Cambridge; the Bristol group welcomed over 400 cryptographers from around the world to the United Kingdom at one of the most successful academic cryptographic conferences ever held.

Undergraduate and MSc. Prizes

Before proceeding to detail our research work, we would first like to congratulate students who did exceptionally well over the year. Three students from the 2010-2011 undergraduate cohort have started PhD’s in cryptography; Peter Scholl (Bristol), Daniel Martin (University of California, San Diego) and James Alderman (Royal Holloway University of London).

Detica Forensics continued their sponsorship of the two annual security prizes in our department: one for the best undergraduate project in the area of security, and one for the best MSc. project in security. The two winners in 2010-11 were:

- Christian Miles, with his undergraduate project on “Multiparty computation; a modern approach” (June 2012). Part of Christian’s thesis makes up a paper we have accepted at the SCN conference later this year.

- Xiaochen Fu, with her MSc. project on “Developing a cryptographic security model for EMV/CAP” (November 2011).

We thank Detica for their continuing support of our programmes.
The Cryptography Group at Bristol has grown considerably in the last year due to us securing a large number of research grants.

**New Post-Docs**

**Ashish Chourdhary**

Ashish secured his Master’s degree from the Indian Institute of Technology (IIT) Madras, India under the supervision of Kamala Krithivasan. He worked on new models of computation, inspired from the DNA computing for his Master’s thesis. During this period he had grown an interest in Theoretical Computer Science and more specifically in theoretic cryptography and decided to join as a PhD student at IIT Madras to work on Cryptography. His supervisor at IIT Madras was Pandu Rangan. For his PhD thesis, Ashish worked on the problem of unconditionally secure message transmission in a distributed setting, where a sender and a receiver are connected by several disjoint paths, some of which can be under the control of a computationally unbounded adversary. He studied the problem in various settings and models, found several interesting lower bound results and developed optimal protocols. He also worked on other problems related to secure distributed computing, such as Verifiable Secret Sharing, Byzantine agreement and secure Multiparty computation. Currently, his focus is on the issues related to the efficiency in MPC protocols in various settings.

**Anna Lisa Ferrara**

Anna Lisa became interested in the fields of cryptography and information security after attending a course on applied cryptography and network security during her undergrad studies at the University of Salerno (Italy), where, thereafter, she received both her Master’s degree and PhD in Computer Science. After graduation, she has continued her academic career as associate researcher first at the Johns Hopkins University, and then at the University of Illinois at Urbana-Champaign. Anna Lisa’s main stream of research concerns the design and analysis of cryptographic protocols with particular emphasis on efficiency requirements and provable-security. She has worked on several topics such as secure signatures schemes, certified email protocols, payment schemes and key assignment, paying particular attention to cryptographic enforcement of access control policies. Recently, as evidenced by her latest works, she has also got interested in automated methods for the verification of security properties of real world protocols.

http://www.cs.bris.ac.uk/Research/CryptographySecurity
Marcel Keller

Marcel studied mathematics at ETH Zurich, where he already developed an interest in cryptography and information security, attending courses ranging from number theory to network security. He concluded his studies with a diploma thesis with Ueli Maurer on private information retrieval. After working for a year as a software developer in industry, he started his PhD at Aarhus University under the supervision of Ivan Damgård. During this study, he worked on several subtopics within the area of cryptographic protocols such as zero-knowledge proofs and multi-party computation. A common theme in his research is creating more efficient protocols by utilizing algebraic properties of the mathematical objects involved. Shortly after handing in his dissertation, he started as a research assistant here in Bristol. Since then he has worked on an implementation of AES in MPC based on FHE, resuming his first project as a PhD student, which was before the advent of FHE.

Georgios Oikonomou

George received the MSc. and PhD degrees in Computer Science from the Athens University of Economics and Business, Athens, Greece, in 2002 and 2009 respectively. His doctoral research contributed a framework for the web-based management of distributed services and systems. Before joining the University of Bristol, he was a Post-Doc Research Associate with Computer Science, Loughborough University, UK. His current research focuses on network and mobile device forensic analysis. He is also interested in network protocols and security for the “internet of things”, with emphasis on IPv6 networking for low-power, severely constrained devices. In the past, he has designed and developed novel multicast forwarding algorithms and congestion control mechanisms for 6LoWPAN networks. He is an active developer of the Contiki open source embedded operating system for the “internet of things”.

http://www.cs.bris.ac.uk/Research/CryptographySecurity
Emmanuela Orsini

Emmanuela studied mathematics in Pisa, Italy, where she received her MSc. with a thesis in computational commutative algebra. After a postgraduate Master’s degree and a period at STMicroelectronics, she started her PhD in mathematics and statistics for the computational sciences at the University of Milano under the supervision of Teo Mora and Max Sala. During that time she was mainly interested in the applications of commutative algebra to coding theory. In March 2008 she moved again to the University of Pisa as a postdoc. Here she began working in cryptography with Carlo Traverso and taught many courses for undergrads in mathematics and engineering. Her research interests include computational algebra, algebraic number theory, coding theory, lattice-based cryptography and fully homomorphic encryption, as well as their mutual interactions.

Gaven Watson

Gaven obtained his MSc. in Mathematics from Royal Holloway University of London in 2006. Following this he remained there to complete a PhD under the supervision of Kenneth Paterson. His thesis examined how to provide formal security analyses of protocols taking into account how they are actually used in practice. The thesis focussed on the CBC mode of operation and the widely used network protocol SSH. During 2011 Gaven was a PostDoc in the iCORE Information Security Lab at the University of Calgary, Canada. During his time in Calgary he examined aspects of cloud computing security.

New PhD Students

Panagiotis Andriotis

Panagiotis Andriotis received the BSc. degree in Mathematics from the National Kapodistrian University of Athens, Greece, in 2006, and the MSc. degree with Distinction in Computer Science from the University of Bristol, United Kingdom in 2012 with a Master’s thesis on Steganalysis of jpeg images using Benford’s Law under Theo Tryfonas. He is currently a PhD student at the University of Bristol. His research interests include Network Security and Computer Forensics. He has worked as a Mathematics teacher in the secondary education in Greece and he is currently working for the inter-university ForToo (Forensic Tools) project.
Valentina Banciu

Valentina is a graduate of the Information Security MSc. Programme organised by the Military Technical Academy of Bucharest. She has also studied Physics at the University of Bucharest in parallel, and holds a second MSc. degree in Theoretical Physics. Valentina is currently working under the supervision of Elisabeth Oswald. Her main topic is physical security of lightweight ciphers.

Gareth Davies

Gareth gained an undergraduate Master’s degree in mathematics from Nottingham University in 2011 and joined the Bristol cryptography group soon after. His work towards his Master’s dissertation investigating elliptic curves and their use in cryptography, under the supervision of Christian Wuthrich, inspired him to pursue academic research in the field. He is currently investigating key agility under the supervision of Martijn Stam and Bogdan Warinschi, with early focus on key-dependent messaging.

Enrique Larraia

Enrique studied mathematics at UCM in Madrid, Spain. By the end of his licenciature, he became interested in Cryptography. In 2010 he was accepted by Royal Holloway University of London and gained a MSc. with distinction. His Master’s thesis was on Braid Cryptography. He just started his PhD studies under the supervision of Nigel Smart. His area of interest is Fully Homomorphic Encryption and Multiparty Computation.

Luke Mather

Luke graduated with a first-class MSci. in Mathematics and Computer Science from the University of Bristol in 2010. He spent a year working as a systems engineer, before returning to Bristol in July 2011 to pursue a PhD under the supervision of Elisabeth Oswald. Luke’s research is in the area of side-channel attacks, in particular the application of side-channel analysis to systems for which anonymity and privacy are important features. The initial focus of his work is on the detection of privacy vulnerabilities in web applications.
Welcome to the new members of our research group:

**Peter Scholl**

Peter completed his MEng in Mathematics and Computer Science in Bristol, choosing to undertake a final year project in Cryptography with Nigel Smart. Having enjoyed this initial taste of research, he decided to continue research in the area by studying for a PhD. He has successfully published a paper based on his Master’s project, and is now focussing on the practical and theoretical aspects of Fully Homomorphic Encryption.

**Theodoros Spyridopoulos**

Theodoros studied electrical and computer engineering in Democritus University of Thrace, Greece, where he continued his studies for a Master’s degree in information security and digital forensics. He joined the Group in February 2012 studying for a PhD in System Modeling Techniques of Cyber Security under the supervision of Theo Tryfonas. The key objective of his research is to examine novel pathways for improving situational awareness in the context of critical information infrastructure, under the premise of Systems Thinking.

**Joop van de Pol**

Joop received a MSc. cum laude in Industrial and Applied Mathematics from the Eindhoven University of Technology under Benne de Weger. For his Master’s thesis, he examined the security of lattice-based cryptography in practice and he will continue this line of research under the supervision of Nigel Smart. This research will help in understanding the security of Fully Homomorphic Encryption schemes.
Over the year we hosted a number of international visitors working on various aspects of cryptography and security.

**Kallia Anastasopolou (U. Aegean, Greece)**

Kallia Anastasopolou joined us under an Erasmus training agreement from February to June 2012. We are developing with her a game theory model of electronic transactions over cloud infrastructure and look into the implications of various privacy preservation strategies in that context.

**Sasha Boldyreva (Georgia Tech., USA)**

Sasha Boldyreva visited in March 2012 as part of a series of exchange visits between Georgia Tech and the Bristol group. We discussed symmetric searchable encryption as a way to speed up search and generalizations to other data-structures.

**Dario Fiore (ENS Paris, France)**

Dario Fiore visited in November 2011 and continued our existing work on pseudofree groups based on the CDH assumption and application of PFGs to verifiable outsourced computation.

**Pooya Farshim (TU Darmstadt, Germany)**

Pooya Farshim visited Martijn in December 2011 and June 2012. They continued their work on the interaction between keys and messages in security notions of primarily symmetric primitives. They were joined in their work by Susan Thomson who visited from Royal Holloway University of London.

**Cedric Fournet (Microsoft Research, UK)**

Cedric Fournet visited in November 2011 as part of our industrial advisory board meeting. He stayed around a little longer and gave a seminar on “Modular Code-Based Cryptographic Verification”, and discussed compositability issues in security definitions, the security of the TLS protocol as well as automatic verifiability of real implementations for cryptographic protocols.

**Adam O’Neill (Boston University, USA)**

Adam O’Neill visited our group in March 2012. He gave a seminar on “Security Notions For Functional Encryption”. Moreover, Adam worked with Georg on public-key encryption with non-interactive opening.
VISITORS

Kenny Paterson (Royal Holloway University of London, UK)

Kenny Paterson visited in September 2011 in the context of Steve William’s viva. Additionally, he worked with Martijn on encryption in the presence of ciphertext fragmentation (which led to a joint Eurocrypt 2012 article).

Olivier Pereira (Université Catholique de Louvain, Belgium)

Oliver Pereira visited in October 2011, giving a seminar on “Running Mixnet-Based Elections with Helios”. During his visit we discussed security definitions for vote privacy and investigated necessary and sufficient conditions for ballot privacy.

Tom Shrimpton (Portland State University, USA)

Tom Shrimpton visited Bogdan and Martijn in December 2011. Together they worked on modelling secure cryptographic APIs and how to implement secure versions with a simple policy using standard cryptographic primitives. Tom will be visiting again in July 2012.

Francois-Xavier Standaert (Université Catholique de Louvain, Belgium)

Francois-Xavier Standaert visited Elisabeth and Carolyn in October 2011 to progress joint work on generic side-channel analysis. This collaboration produced a paper which is currently in submission.
**Eurocrypt 2012**

As already remarked we hosted the Eurocrypt conference in Cambridge in April 2012. As well as a packed programme of general talks, including two co-authored by Bristol researchers; the rump session was this year chaired by Martijn Stam. Martijn made it a particularly British themed affair having a “Cryptographic Pub Quiz” as part of the proceedings. The conference was rounded off with a trip to Bletchley Park and a tour of The National Museum of Computing.

**Cambridge Workshops**

As well as organizing Eurocrypt we also organized two other workshops in Cambridge as part of the 100th anniversary of the birth of Alan Turing. The first of these on “Is Cryptographic Theory Practically Relevant?” brought together a number of researchers from both industry and academia; and an audience of well over 100 people. The event was considered a great success and a follow up workshop is now planned for next year, and to be held at Stanford University in the heart of silicon valley.

The second workshop on “Formal and Computational Cryptographic Proofs” focused on more theoretical aspects of cryptography; and attracted a set of leading speakers including Goldwasser, Micali, Maurer, Pointcheval and Rogaway.

**ACE-CSR**

The Bristol Cryptography group was the lead group in obtaining Academic Centre of Excellence in CyberSecurity for the University of Bristol. This status means we are going to work more closely with EPSRC and GCHQ in future. Along with Bristol seven other institutions were given this status.

**Georgia Tech Exchanges**

We initiated, with the help of the British Consulate in Atlanta, Georgia a series of exchange meetings with Georgia Tech. As well as Sasha Boldyreva visiting Bristol, Martijn, Nigel, Bogdan and Joop all spent some time in Atlanta discussing research plans and ideas with the group at Georgia Tech.

**IACR Board**

Nigel Smart was elected to the IACR Board of Directors in November 2011; where he joins Martijn Stam who is the current IACR Secretary.
In the 2011 calendar year we published a record of 34 papers, on a variety of topics in cryptology as a group. Of the IACR venues we published two papers each at Eurocrypt, Asiacrypt, Crypto, and CHES; and one paper in PKC and the Journal of Cryptology. In addition we branched out into publication at the top security conferences; with two papers at ACM-CCS and one at ESORICS.

The papers covered various areas including (but not limited to):

- Analysis of important real world protocols such as SSL/TLS and SSH.
- Hash functions
- Fully homomorphic encryption.
- Secure processor architectures.
- The Helios e-voting protocol.
- Statistical analysis in DPA/SCA attacks.

Our co-authors consisted of people from various countries; including Austria, Belgium, China, Finland, France, Germany, India, Ireland, Italy, Japan, Korea, Luxembourg, and Switzerland. In addition we published papers with a variety of co-authors from different companies; including Gemalto, Hewlett-Packard, and ST-Ericsson.
Finally, looking back on our papers published in 2010 we find (via Google Scholar) that four have already achieved a significant number of citations:


These citation counts were computed in June 2012.

Below you can see a photo of those of the group who attended Eurocrypt 2012:
**Work on the Helios e-voting system**

Helios is a cryptographic voting protocol that has been used in practice. In 2011, Cortier and Smyth discovered potential issues in Helios that could lead to a compromise of voters’ privacy. We developed a security model for voting to formalise privacy. At ESORICS 2011, we presented our model and some possible adaptations to Helios making it provably secure in our model. These adaptations, however, reduced the efficiency of ballot creation and verification. This year, we have improved our analysis and can propose changes to Helios which attain provable security while incurring no significant extra cost in terms of efficiency. We have also explored an alternative formalisation of privacy based on notions of entropy and established relationships between this method and our cryptographic model.

**Hash Functions**

Hash functions are one of the fundamental cryptographic primitives. One popular way to construct a hash function is to add a wrapper to a blockcipher so it satisfies the basic requirements of a hash function. Recent work has concentrated on so-called double-length constructions, where a compression function is created that outputs twice as many bits as the underlying blockcipher.

Tandem-DM is a well-known construction of this type, yet a decent analysis of its provable properties was missing until recently. In two articles, we addressed the collision resistance (Crypto’11) and preimage resistance (Asiacrypt’11) of Tandem-DM and other related constructions. From a practical perspective, a comprehensive efficiency analysis and comparison of many different compression functions (including Tandem-DM) was made when using AES and exploiting the AES instruction set extension for CPUs (CHES’11).

An important challenge in the design of compression functions are double-length constructions based on blockciphers with relatively small keys. We presented an elegant construction (TCC’12) based on incidence geometry that achieves a desirable efficiency/security tradeoff, thereby filling a gap in the literature.
Cryptography and Information Security Research

for further information contact:

Professor Nigel Smart
University of Bristol
Department of Computer Science
Merchant Venturers Building
Woodland Road
Bristol BS8 1UB
UK

http://www.cs.bris.ac.uk/Research/CryptographySecurity/

BristolCrypto