University of
BRISTOL

INTRODUCTION

In the 2009-10 academic year, Cryptography research at the University of Bristol went from strength to strength; It has been a busy year with growth in the group, and more growth to come in 2010-11. In addition, we have produced a number of research results which have made an impact on the world stage. As usual, the work encompasses a combination of practice and theory, which makes Bristol a unique environment in which to conduct cryptographic research. In this report we overview a number of highlights and changes which have occurred.

As usual, we presented our work and attended a number of conferences and meetings, these included Asiacrypt (Tokyo), CryptoForma (Paris and Kent), CARDIS (Passau), Eurocrypt (Monaco), PKC (Paris), PQCrypto (Darmstadt), and SCN (Amalfi),

You can keep track of where we are visiting and news in the group, via our new Twitter account *BristolCrypto*.

The major news item, in the longer term, is that we will be organizing Eurocrypt 2012 in Cambridge. This is especially significant since 2012 marks the 100th anniversary of the birth of Alan Turing. In addition we are involved in organizing a six-month programme at the Newton Institute in the same year, and we are also involved in organizing a Dagstuhl workshop on *Security in the Cloud* scheduled for December 2011.

Undergraduate and MSc Prizes

Before proceeding to detail our research work, we would first like to congratulate students who did exceptionally well in the last year. Each year Detica Forensics sponsors two 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 the 2009-10 academic year were:

- Luke Mather, who won the undergraduate prize in June 2010 for his project on "*The multivariate Kolmogorov-Smirnov test in differential power analysis attacks*".
- Emili Evripidou, who won the MSc prize in November 2009 for her project on "*Practical eVoting based on extensions to the Paillier encryption scheme and zero-knowledge proofs*".

We thank Detica Forensics for their continuing support of our programmes.

As well as project work in the department students, on our undergraduate and masters programmes, have the opportunity to study cryptography and security in three units "Introduction to Cryptography", "Advanced Cryptography" and "Information Security". Aspects of security and cryptography are also touched on in a number of other units in all our degree programmes.

NEW STAFF

The Cryptography Group at Bristol has grown considerably in the last year. This has mainly been due to us obtaining funding for our research via a number of new EPSRC grants.

New RA: Stefan Tillich

During his Master studies at the Graz University of Technology, the two topics of hardware design and security became his primary interest. Naturally, his PhD work was centered around these topics, focusing especially on embedded systems. In Stefan's PhD work he addressed the predominant challenges faced by the ever growing number of embedded systems deployed today: security on the one side and efficiency on the other. Security is a natural requirement of many computing applications, since digital data sent in today's networks is inherently prone to eavesdropping, replication, and manipulation. On the other hand, embedded systems have limited resources and certainly cannot waste them by executing heavy-weight security algorithms. His PhD work started out with an investigation of efficient implementation of security workloads, and gradually moved towards solutions for physically secure implementation of such workloads. After his PhD he continued his research in this area as a post-doctoral researcher at Graz University of Technology; this work will be extended now he has joined the University of Bristol. Our current ambitious research goal, which builds on Stefan's track record, is to design and build an embedded processor which both allows to secure the whole embedded system with robust security algorithms in an efficient manner, and at the same time fend off the dreaded implementation attacks. The concepts developed and tested today will serve as a "blueprint" for future secure embedded devices.

New PhD Students

As well as Stefan, five new PhD students started:

- Simon Hoerder and Marcin Wojcik, who are working on hardware designs for protecting against side channel attacks.
- Ming-Feng Lee, who is working on group signatures.
- Jake Loftus, who is working on security for cloud computing.
- Carolyn Whitnall, who is working on statistical analysis techniques for extracting data from power traces.

People Leaving

As well as people arriving, three people have left:

- Johann Großschädl, who has obtained a post-doctoral position at the University of Luxembourg.
- Andrew Moss, who has joined BTH (Sweden) as a Lecturer.
- Paul Morrissey, obtained his PhD and has now taken up a position at Hazell Carr, part of Xafinity Ltd.

GRANTS OBTAINED

As well as continued funding from existing grants and awards from EPSRC, the Royal Society and the European Union, the group has secured a number of new funding streams in the last twelve months.

Architectural and Micro-architectural Countermeasures against Physical Attack

A modern computer processor is usually general-purpose: this means it can execute any program, rather than just a single, specific one. On one hand, this is tremendously useful; for example it means we do not need one computer to run our web-browser and another computer to run our word processor! On the other hand, there is no "free lunch": by being general-purpose, the processor often misses the opportunity to deal effectively with a specific program (or class of programs). For example if one were to build a computer dedicated to executing web-browsers, one might expect it to be better at this specific task because that's all it does. Placed in the context of security, this issue starts to become more of a problem. Specifically, some decisions made during the design of general-purpose computer processors imply the possibility of security vulnerabilities: because the computer cannot cater for the specific needs of a security critical program, it might actually "help" an attacker to break said security. Our EPSRC funded project aims to investigate this problem from a number of different perspectives. The grant, for £823,396, started in October 2009 and enables us to work on these issues with our existing partners at AIST (Japan), SiVenture (UK), Cryptography Research Inc (USA) and XMOS Ltd (UK).

Privacy and Attestation Technologies

Digital signature schemes are a way of signing digital documents. However, a major disadvantage is that such signatures uniquely identify the signer. This is a disadvantage in applications where one does not care that a specific person signed a document, only that they are part of some specific group (for example they are a manager of a company). One can create signature schemes, called group signatures, with the property that they enable the member of a group to sign whilst maintaining the signers anonymity. The project aims to develop new and more efficient ways of producing group signatures, and an associated concept called Direct Anonymous Attestation (DAA). These protocols are currently deployed on the Trusted Platform Module chip which is included on most computer motherboards. By developing new methods for constructing such schemes, we hope to enable more efficient protocols which can be used to enhance user privacy when surfing the Internet. The grant from EPSRC of £497,178 was awarded in Spring 2010, and the project will start in October 2010. This project enables the group to continue its existing work in this area with Hewlett-Packard Laboratories (UK), IBM Labs (Switzerland) and Trend Micro (UK).

GRANTS OBTAINED

Cloud Computing and Secure Databases

Focusing on security aspects of cloud computing, and funded by a CASE award from EPSRC and Trend Micro, this project started in October 2009. Its aim is to work out how one can secure the applications and data which are being outsourced to cloud computing providers. Cloud computing provides a major step change in the way companies are dealing with their computing requirements: it promises major benefits in terms of scalability and cost, yet comes with equally large concerns with respect to security.

Google Faculty Research Awards Programme

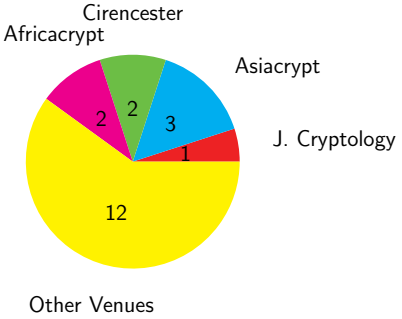
As part of Google's Faculty Research Awards Programme, we have been awarded a grant to build on the group signature and DAA work mentioned above, as well as other anonymity preserving technologies. The award will enable us to part-fund PhD students who are currently working on these topics.

EPSRC Leadership Fellowship

Finally, Elisabeth Oswald has been awarded a prestigious EPSRC Leadership Fellowship worth $£1,083,542$. This five-year fellowship will enable Elisabeth to expand on her existing side-channel security laboratory. The fellowship, entitled "*SILENT: Side-channels – theory and implications for society*" will start in January 2011, and will look at a number of aspects of side-channel analysis. First, it will investigate the theoretical underpinnings of how practical attacks are carried out, and the defences one can use to mitigate these attacks. It will then go on to see how these techniques can be transferred to other domains where observations of emitted data can be used to determine private information; for example, applications such as Facebook where users may not realise that the public data they publish may allow attackers to determine data that they would rather keep private. The project involves partnerships with Microsoft Research (UK), Infineon Technologies (Germany), RFI Global (UK) and the University of Louvain (Belgium).

PUBLICATION OVERVIEW

In the 2009 calendar year we published twenty papers, on a variety of topics in cryptology as a group.



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

- Hardware-based protection against side channel attacks. In particular analysis of our NONDET design on an FPGA.
- A mechanism to distribute the key generation centre for Sakai-Kasahara ID-based encryption schemes. This work was performed to solve a real world problem encountered by Trend Micro.
- A formal security model for client puzzles, a proposed form of defence for web sites against distributed Denial-of-Service (DDoS) attacks.
- An analysis of Schnorr signatures in the generic group model. This work was conducted to help the ongoing standardization work for Schnorr signatures in ISO.
- Domain-specific compilers and languages for cryptography. This work aims to enable non-expert programmers to build cryptographic systems which are as efficient as if they were built by experts.

Finally, looking back on our papers published in 2008 we find (via Google Scholar) that four have already achieved a significant number of citations:

- S. Galbraith, K.G. Paterson, N.P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, **156**, 3113–3121, 2008. (141 Citations).
- K. Bentahar, P. Farshim, J. Malone-Lee, N.P. Smart. Generic constructions of identity-based and certificateless KEMs. *Journal of Cryptology*, **21**, 178–199, 2008. (78 Citations).
- Y. Lindell, B. Pinkas, N.P. Smart. Implementing two-party computation efficiently with security against malicious adversaries. *Security and Cryptography for Networks 2008*, Springer LNCS 5229, 2–20, 2008. (29 Citations).
- M. Abadi, B. Warinschi. Security analysis of cryptographically controlled access to XML documents. *Journal of the ACM*, **55**, 1–29, 2008. (27 Citations).

These citation counts were computed in July 2010.

RESEARCH HIGHLIGHT: FULLY HOMOMORPHIC ENCRYPTION

For nearly 30 years, one cryptographic dream has been to come up with an encryption scheme for which you can 'add' and 'multiply' ciphertexts, i.e., a so-called fully homomorphic scheme. This means that given two ciphertexts c_1 and c_2 which encrypt messages m_1 and m_2 under a key k, i.e.

$$c_1 = \mathsf{Enc}(k, m_1)$$
$$c_2 = \mathsf{Enc}(k, m_2)$$

there is an operation Add, which produces a ciphertext c_3 that corresponds to the encryption of $m_1 + m_2$. Also there is an operation Multiply which produces a ciphertext c_4 that is the encryption of $m_1 \times m_2$.

$$c_3 = \mathsf{Add}(c_1, c_2) \quad = \mathsf{Enc}(k, m_1 + m_2),$$
$$c_4 = \mathsf{Multiply}(c_1, c_2) = \mathsf{Enc}(k, m_1 \times m_2).$$

The important point is that to apply Add and Multiply we do not need knowledge of the key k, or the messages m_1 and m_2, and so anyone can apply them.

So what is the big deal about Add and Multiply? Well as soon as you can Add and Multiply you can compute *any* function! For example, suppose you are engaged in an online auction, you could encrypt your bids to the auctioneer, but maybe you do not trust the auctioneer to find out what your bid is. Maybe the auctioneer could use this to cheat and encourage higher bids to increase his commission. Using a fully homomorphic scheme the auctioneer could work out who won, and what the winning bid was, without learning what all the other bids were. As another example, you could encrypt your vote in an online election and then the central authority could work out who won the election, without learning anything about the votes of the individual voters; voter privacy would thus be ensured.

Over the years, many encryption schemes have been proposed which either have the Add operation *or* the Multiply operation, but not *both*. In 2009, Craig Gentry (IBM) came up with the first scheme which simultaneously allows you to Add and Multiply ciphertexts; Gentry's scheme was a major theoretical breakthrough.

In a paper, presented in May at the *PKC 2010* conference in Paris, Nigel Smart (Bristol) and Frederik Vercauteren (KU Leuven and ex-Bristol) devise a way of simplifying Gentry's scheme so that it becomes more practical. While the new scheme is not fully practical, (in the sense that it could be used in a real-life application) it is an important step toward the formation of a system which is practical.

Smart and Vercauteren's scheme also provides an intriguing new application of objects in an area of Pure Mathematics called class groups of number fields. Such objects have been studied in Pure Mathematics for around two centuries with little possibility of impact on everyday life; this work is therefore another example of the unexpected applicability of decades of curiosity-driven research.

OTHER RESEARCH HIGHLIGHTS

At Asiacrypt 2009 in Tokyo last year we presented three papers on very different aspects of cryptography:

Security Notions and Generic Constructions for Client Puzzles.

This paper discussed a defence for websites against attackers who launch denial-of-service attacks. Such attacks are becoming more common on the internet, with high-profile attacks taking place against many leading websites. The paper, from research by Bristol University academics, Paul Morrissey, Nigel Smart, Bogdan Warinschi (all from bristol University) and Liqun Chen (Hewlett-Packard Laboratories in Bristol), investigated a specific defence technique that aims to make performing such attacks computationally infeasible, while not overburdening the innocent user.

Secure Two-Party Computation is Practical.

In this paper, which represents joint research between Nigel Smart and Steve Williams (Bristol University); Benny Pinkas (University of Haifa, Israel) and Thomas Schneider (Ruhr-University at Bochum, Germany), the team showed that a procedure thought to be only theoretical can actually be implemented in practice. One goal of this collaboration is to ultimately create another method for databases to compute on encrypted data. Future applications of this research could allow doctors to access centralised healthcare databases in a way that protects patient confidentiality.

Foundations of Non-Malleable Hash and One-Way Functions.

In the final paper by Bogdan Warinschi (Bristol University); Alexandra Boldyreva and David Cash (Georgia Institute of Technology, USA) and Marc Fischlin (Technical University in Darmstadt, Germany), the researchers considered foundational issues related to basic constructions in cryptography. This research is an important step in understanding the properties of a cryptographic object called a "random oracle". Such objects are a popular solution in constructing efficient cryptographic schemes, such as those used in a web browser.

Asiacrypt is held annually in a different city in the Asia-Pacific region and is one of the three flagship conferences of the International Association for Cryptologic Research. The other two conferences are: Crypto, held annually in Santa Barbara California, and Eurocrypt held annually in a different European city.

Nigel Smart, Professor of Cryptology in the Department of Computer Science at the University of Bristol and co-author on two of the papers, said: "We are delighted to have such a strong presence at 2009's Asiacrypt conference, especially as it was particularly hard to have papers accepted. Of 300 submissions, just over 40 were selected for presentation at the conference."

IMPACT

The group continues to engage with stakeholders so as to maximize the impact of our work in the world.

eCrypt-2: Algorithm and Key Size Report:

This year we oversaw a major update to the annual "Algorithm and Key Size" report of the eCrypt-2 Network of Excellence. This report details the recommendations and advice of a number of leading European research groups in relation to the selection of algorithms and parameters for practical deployment. Whilst having been produced on an annual basis since 2004, the 2010 update includes a number of new sections and substantially rewritten advice.

In particular the report now covers further updates on the attacks against the standard hash function algorithms, a major new section on key agreement protocols, a more elaborate discussion of hybrid encryption schemes, as well as updates on the efficiency of hardware and software based cryptanalytic efforts. In addition we continue the line taken in the 2009 report of recommending only using 80-bit security levels (i.e. 1024-bit RSA and 160-bit ECC key sizes) for legacy applications. Our recommendation is that new systems move to 128-bit symmetric key security levels (i.e. roughly 3072-bit RSA and 256-bit ECC key sizes).

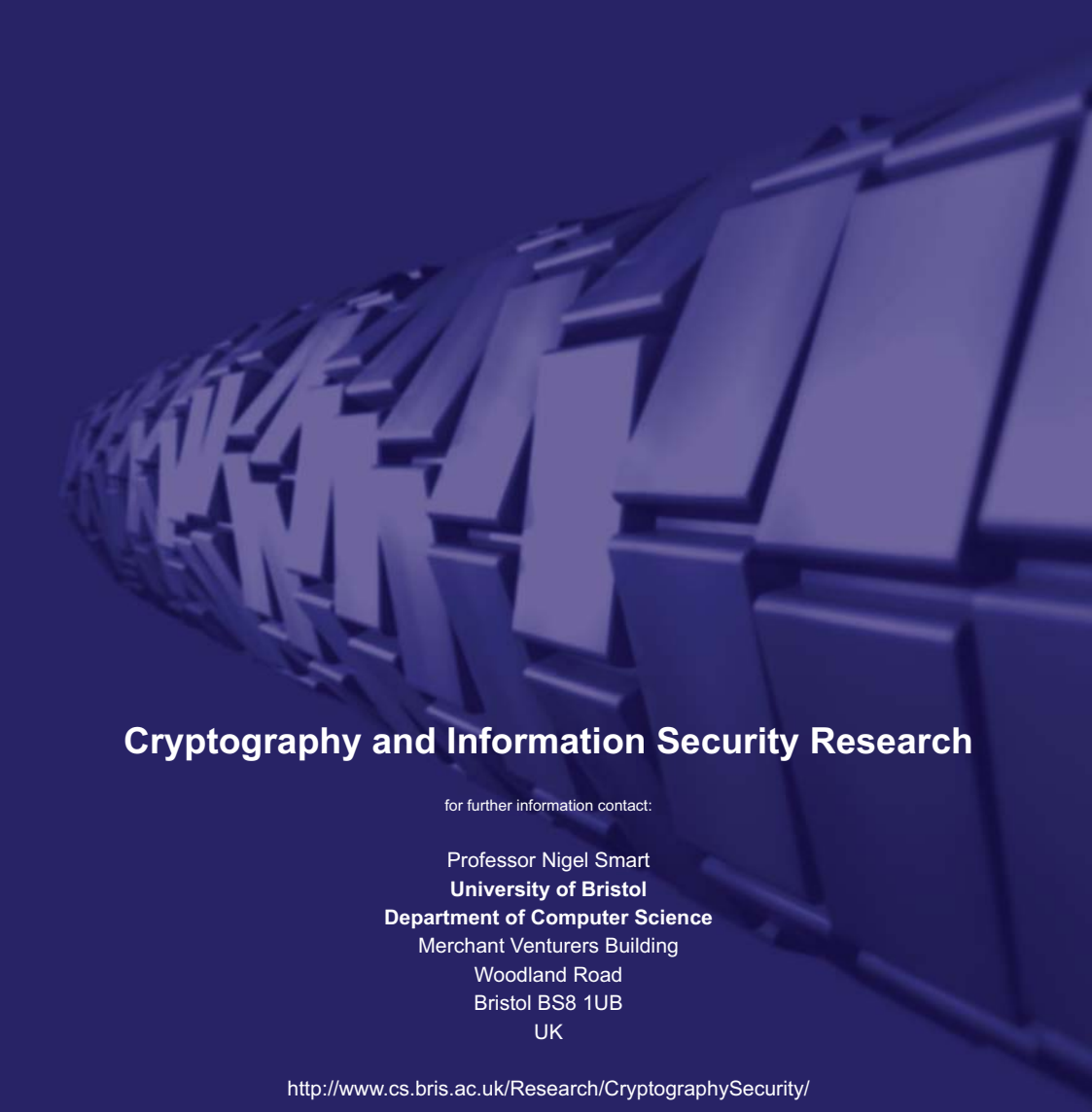
The report can be downloaded from the following web site:

http://www.ecrypt.eu.org/

IEEE 1363.3: Pairing Based Cryptography:

The IEEE 1363.3 standard is now nearing completion and the Bristol group has been actively involved in helping draft the new standard. This standard will be the first major standard on pairing based cryptography; a technology which allows various new forms of encryption and signature methodologies, such as identity-based encryption.

In particular the new standard will include a number of Bristol based contributions in the area; including the Sakai–Kasahara based Key Encapsulation Mechanism for identity-based encryption (the SK-KEM algorithm), a variant of the Smart–Chen–Kudla identity-based key agreement protocol, as well as efficient pairing algorithms based on the Ate-pairing and it's extensions.



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