ISG Research Seminars August 2006 – June 2012

28th June **Youn Chan Jung** (University of Korea): TBC

23rd May **Vassil Dimitrov** (University of Calgary): Inversion over binary fields

22nd May **Vassil Dimitrov** (University of Calgary): Loading the bases II

21st May **Vassil Dimitrov** (University of Calgary): Loading the bases I

8th May **Stefano Zanero** (Politecnico di Milano, NECST Lab): iSnoop: how to steal secrets from touchscreen devices

1st May **Federico Maggi** (Politecnico di Milano, NECST Lab): The long story of short URLs: a user-centric, large-scale measurement

26th April **SeongHan Shin** (ISG, RHUL): Introduction to leakage-resilient authenticated key exchange (LR-AKE)

29th March 2012	**Speaker:** Tibor Jager (KIT Karlsruhe) **Title:** A Standard-Model Security Analysis of TLS-DHE (joint work with Florian Kohlar, Sven Schäge, and Jörg Schwenk) **Abstract:** TLS is the most important cryptographic protocol in use today. However, up to now there is no complete cryptographic security proof in the standard model, nor in any other model. We give the first such proof for the TLS ciphersuites based on ephemeral Diffie-Hellman key exchange (TLS-DHE), which include the cipher suite TLS DHE DSS WITH 3DES EDE CBC SHA mandatory in TLS 1.0 and TLS 1.1. Due to subtle problems with the encryption of the final Finished messages of the TLS handshake, this proof cannot be formulated in the Bellare-Rogaway (BR) or any other indistinguishability-based model. Therefore we only prove the security of a truncated version of the TLS handshake (which has been the subject of all previous papers on TLS except [34]) completely in the standard BR model. We then define the notion of authenticated and confidential channel establishment (ACCE) as a model in which the combination of TLS handshake and TLS Record Layer can be proven secure. Eprint is available here.
22nd March 2012	**Speaker:** **Claire Vishik** (Intel) **Title:** Trust Evidence: Defining the Next Generation of Trusted

Computing Projects

Abstract: Dynamic electronic communications in today's heterogeneous environment require systems to generate, transmit, receive, process, and consume "trust evidence" in order to manage security risks. To improve security, systems need to be able to:

1. Establish whether a peer device, network, or system is trustworthy. Currently, authentication is the only approach commonly used to ascertain trust in interactions. The mere fact that a device or user can prove membership in a certain administrative domain is typically sufficient to gain access. Such an approach is not viable in a multi-domain environment.

2. Establish the threat posture to assume toward any peer entity in the heterogeneous environment. Currently, the level of trust afforded during interactions is defined as a dichotomy of trusting or not trusting the other party or parties. Identifying more nuanced approaches and determining whether those alternatives have practical value is an open problem.

3. Dynamically measure the degree of trustworthiness in devices and systems as their software and operational environments change. Current approaches and implementations don't work across domains; require significant investment in infrastructure for deployment; and suffer from a variety of other challenges. We need to find a viable, lightweight approach to trust measurement and establish that the approach has value.

4. Discover trustworthy devices, systems, and networks, to ensure optimal risk levels of the common electronic processes. Currently, there are no viable approaches to optimizing processes based on trust establishment with other participants in the process (devices, networks, applications, or users). We need to define methods to establish trusted communications between two entities belonging to different domains, by matching the trust information provided by these entities to the policies of the requestor.

Novel approaches to trust are needed to ensure that protocols, platforms, devices, and common

	applications possess mechanisms to prove their trustworthiness during interactions with other components of the computing environment. We believe that innovative mechanisms are required to allow entities in a heterogeneous environment to manage the risks of communication and collaboration. The talk will discuss our exploratory effort to define Trust Evidence and related issues.
15th March 2012	**Speaker:** Peter Ryan (University of Luxembourg) **Title:** A Brief (Biased) History of Verifiable Voting Schemes: from theory to practice **Abstract:** In this talk I outline recent advances toward secure but usable, verifiable voting schemes. In particular I will outline recent steps in the evolution of the Prêt a Voter polling station scheme as well as the "Pretty Good Democracy" (PGD) internet voting scheme (developed with Vanessa Teague). I will also describe the recent idea of incorporating the confirmation code mechanism of PGD into Prêt a Voter. Finally, time permitting I will describe the "Caveat Coercitor" scheme developed with Mark Ryan.
8th March 2012	**Speaker:** Jacob Schuldt (RCIS - AIST, Japan) **Title:** On the Impossibility of Constructing Efficient Key Encapsulation and Programmable Hash Functions in Prime Order Groups **Abstract:** The construction of chosen ciphertext secure (CCA secure) public key encryption schemes has long been a central research topic in cryptography, and especially the construction of efficient schemes has received a lot of attention. In this talk, we focus on the problem of minimizing ciphertext overhead, and discuss the (im)possibility of constructing key encapsulation mechanisms (KEMs) with low ciphertext overhead. More specifically, we rule out the existence of algebraic black-box reductions from the (bounded) CCA security of a natural class of KEMs to any non-interactive problem. The class of KEMs captures the structure of the currently most efficient KEMs defined in standard prime order groups, but restricts an encapsulation to consist of a single group element and a string. This result suggests that we cannot rely on existing techniques to construct a CCA secure KEM in standard prime order groups with a ciphertext overhead lower than two group elements. Furthermore, we show how the properties of an (algebraic)

	programmable hash function can be exploited to construct a simple, efficient and CCA secure KEM based on the decisional Diffie-Hellman problem with a ciphertext overhead of just a single group element. Since this KEM construction is covered by the above mentioned impossibility result, this enables us to derive a lower bound on the hash key size of an algebraic programmable hash function, and rule out the existence of algebraic (poly, n)-programmable hash functions in prime order groups for any integer n.
9th March 2012	**Speaker:** Yuan Xiang Gu (Cloakware, Irdeto) **Title:** Software Protection and Security Dynamics **Abstract:** What is the most important security challenge for current application systems? The fact that untrusted environments become a part of mainstream consumer devices and cloud computing hosts, and security is a moving target! Digital content consumed via commodity devices is penetrating every aspect of life, along with other advanced Internet-based and wireless technologies. Modern security is facing new challenges because traditional perimeter defenses against man-in-the-middle attacks are inadequate protection against the man-at-the-end white-box attacks favored by many attackers. Recently, homomorphic encryption research is receiving serious attention. In fact, the security issues, which can be addressed by homomorphic encryption, have also been addressed by data transformations that constitute a part of software protection technologies. In this presentation, we will discuss White-Box attacks and vulnerability in real world and why software protection is important. We also provide an brief introduction to software protection technology and software security lifecycle management.
1st March 2012	**Speaker:** Barbara Kordy (University of Luxembourg) **Title:** Security modelling using attack-defence trees **Abstract:** Attack trees are a well-known and widely used methodology to describe the possible security weaknesses of a system. However, there are several important aspects of security that attack trees cannot model. Besides the fact that the attack tree formalism only considers the attacker's point of view, it can neither capture the interaction between an attacker and a defender, nor is it well-suited to depict the evolution of attacks and subsequent defences. In order to overcome these limitations, we extend attack trees with defence nodes. Therefore, we define

	attack-defence trees where attack and defence nodes may appear at any level of the tree. This richer formalism allows for a more precise modelling of a system's vulnerabilities, by representing interactions between possible attacks and corresponding defensive measures. This talk will give an overview of the attack-defence tree methodology. After introducing the syntax as well as possible semantics for attack-defence trees, a number of interesting questions, including equivalent representations of security scenarios, quantitative analysis using attack-defence trees and computational complexity of the considered model, will be discussed.
23rd February 2012	**Speaker:** James Heather (University of Surrey) **Title:** What have we ever done for the Victorians? **Abstract:** We now have a wealth of secure voting system designs that can cope with traditional elections: a flat list of candidates, and a first-past-the-post tallying method. Unfortunately, real elections are often considerably more complex, and somewhat arcane. We discuss our current work on building a prototype system for the state of Victoria, Australia, and how to adapt the theory to fit the practice.
9th February 2012	**Speaker:** Tom Chothia (University of Birmingham) **Title:** Using Information Theory and Statistics to Measure Information Leaks **Abstract:** In this talk I will describe how information theory can be used to quantify information leaks from secure systems, and how these measures can be estimated from trial runs of a system. Information theory provides meaningful definitions of leakage that can be applied in a wide range of situations, and using statistical estimation makes it possible to use these techniques to test implemented systems. As an example, I'll discuss a time-based traceability attack against the RFID chip in e-passports. This is joint work with Kostos Chatzikokolakis and Apratim Guha
2nd February 2012	**Speaker:** Steve Schneider (University of Surrey)

	Title: Write-ins for Pret a Voter **Abstract:** This talk presents an extension of the Pret a Voter verifiable voting system to handle write-ins: an additional option on the ballot form to cast a vote for any person by writing in their name. Write-ins are common in the U.S. as part of the electoral landscape. They pose a particular challenge for end-to-end verifiable voting systems, since receipt-freeness and coercion-resistance are key requirements that do not sit well with write-ins. This talk presents the extension to Pret a Voter to allow write-ins, retaining the ability of a voter to retain a record of what was cast. The system also provides flexibility with respect to the tallying of write-in votes. We consider the system against the key security requirements and show that they can be achieved with the strongest version of the system.
26th January 2012	**Speaker:** Lorenzo Cavallaro (ISG, RHUL) **Title:** A beautiful journey **Abstract:** From memory errors and countermeasures to malware analysis and (intrusion) detection; from OS dependability to hardware-supported virtualization. In this likely unorthodox talk, I will sketch out some of the most interesting and exciting research topics I've come across to date, zooming in, if necessary, into the key aspects of the research, highlighting pros and cons to hopefully foster further and interesting discussion. I will then conclude pointing out upcoming security-related threats and future research directions.
19th January 2012	**Speaker:** Bill Roscoe (University of Oxford) **Title:** Checking noninterference in Timed CSP **Abstract:** A well-established specification of noninterference in CSP is that, when high-level events are appropriately abstracted, the remaining low-level view is deterministic. This is not a workable definition in Timed CSP, where many processes cannot be refined to deterministic ones. We argue that in fact "deterministic" should be replaced by "maximally refined" in the definition above. We show how to automate the resulting timed noninterference check within the context of the recent extension of FDR to analyse a discrete version of Timed CSP and how an extended theory of digitisation has the potential both to create more accurate specifications and to infer when processes are non-interfering in the more usual continuous-time semantics.

12th January 2012	**Speaker:** Gerhard Hancke (ISG, RHUL) **Title:** Improving RFID Protocol Security with Physics **Abstract:** In modern communication systems a communication neighbour can no longer be assumed to also be a physical neighbour, as it is relatively easy to relay legitimate messages between parties. Additional assurance as the authenticity of the parties is therefore needed. In other words, a party must be sure that the device it is communicating with is also the device that generated the message. Similarly, situations arise where a reader might want to verify that a specified group of RFID tags are all located in close proximity at the same time. One possible solution is to bind specific devices to the protocol execution through the use of physical context characteristics, such as properties of the communication channel, the observed environment or the participating parties' physical location. This talk will give a general introduction to approaches incorporating physical characteristics into cryptographic protocols to improve security services, either by providing additional assurance as to authenticity of the participating parties or increased execution efficiency. Secondly, a new protocol that uses intentional communication channel collisions to authenticate of a chosen subset of RFID tags simultaneously is discussed. This is an ongoing research topic within the SCC with the objective of verifying the integrity of a group of RFID tags, e.g. a shipment containing multiple tags, within a limited amount of time.
1st December 2011	**Speaker:** Özgür Dagdelen (Center for Advanced Security Research Darmstadt, Germany) **Title:** Random Oracles in a Quantum World (joint work with Dan Boneh, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry) **Abstract:** The interest in post-quantum cryptography --- classical systems that remain secure in the presence of a quantum adversary --- has generated elegant proposals for new cryptosystems. Some of these systems are set in the random oracle model and are proven secure relative to adversaries that have classical access to the random oracle. We argue that to prove post-quantum security one needs to prove security in the quantum-accessible random oracle model where the adversary can query the random oracle with quantum state. We begin by separating the classical and quantum-accessible random oracle models by presenting a scheme that is secure

	when the adversary is given classical access to the random oracle, but is insecure when the adversary can make quantum oracle queries. We then set out to develop generic conditions under which a classical random oracle proof implies security in the quantum-accessible random oracle model. We introduce the concept of a history-free reduction which is a category of classical random oracle reductions that basically determine oracle answers independently of the history of previous queries, and we prove that such reductions imply security in the quantum model. We then show that certain post-quantum proposals, including ones based on lattices, can be proven secure using history-free reductions and are therefore post-quantum secure. We conclude with a rich set of open problems in this area.
24th November 2011	**Speaker:** Colin Boyd (Queensland University of Technology, Brisbane, Australia) **Title:** Client puzzles for denial-of-service resistant authentication **Abstract:** A puzzle scheme is a mechanism for delaying a party aiming to obtain some service. Among their applications, puzzles are helpful in protecting authentication protocols from denial-of-service attacks. This talk will provide an overview of puzzle properties and their applications, including formal models for their analysis. Different constructions will be surveyed and integration of puzzles into cryptographic protocols considered. Protection of real-world protocols such as TLS and web services will also be considered. This talk will present joint work with Juan Gonzalez Nieto, Lakshmi Kuppusamy, Jothi Rangasamy, Douglas Stebila.
17th November 2011	**Speaker:** Theo Dimitrakos (Head of Security Architecture Research, BT Group CTO, UK) **Title:** A cloud security research and innovation roadmap - emphasis on innovative technologies and challenges for secure IT virtualisation and data protection in the cloud **Abstract:** Cloud computing has emerged as one of the most promising and challenging IT technologies of our time. This new paradigm utilises two separate technological development—utility computing and service oriented architecture—to provide the users (individuals, SMEs and enterprises) with a highly scalable, pay-per-use, everything-as-a-service model for IT delivery. The characteristics of cloud give rise to several business drivers that make cloud computing an attractive service delivery model

	from a customer's point of view. Customer expectations include capital expenditure reduction, increased IT agility, faster return on investment and removal of barriers to entry as well as a more robust and resilient infrastructure leading to improvements on business continuity. However, cloud technology has also brought to forefront questions related to risk, security and trust both from an academic and an industrial perspective. Security is a big consideration when enterprises consider moving their IT processes to the cloud. The perceived loss of control over process and services along with the concerns over confidentiality of corporate data, privacy, integrity and availability of services and data act as significant showstoppers preventing Corporations and SMEs from using cloud based services. In this talk we will 1. Identify some of the major security challenges and aim to provide recommendations, based on the work of international expert groups by the European Network and Information Security Agency and the Cloud Security Alliance among others 2. Summarise the research and innovation roadmap put forward by BT Research & Technology for addressing -- the security of BT's virtual data centres and emerging cloud infrastructures, -- the security of data and applications services in the cloud -- the secure corporate use of 3rd party cloud infrastructures and services -- issues related to a provider offering security services via a cloud delivery model 3. Elaborate on selected solutions for relating to virtualisation security and cloud data security 4. Highlight challenges for further research and collaboration opportunities with academia.
10th November 2011	**Speaker:** Carroll Morgan (University of New South Wales, Sydney, Australia) **will give *two talks:*** **Talk A (11am):** Semantics for noninterference security: Rhyme and Reason *(joint work with Annabelle McIver and Larissa Meinicke)* **Abstract:** The Shadow model for qualitative noninterference security of sequential programs [1] is a denotational model, complete with a refinement relation that preserves both functional- and security properties (the latter within its terms of reference). It was derived from a series of "gedanken"

experiments in program-refinement algebra, then applied to Kripke structures as used for logics of knowledge.

The Hyperdistribution model for quantitative noninterference [2] was later constructed with the Shadow in mind, but essentially independently. It turns out to have strong structural links to Hidden Markov Models.

The technical component of this talk will be to describe the two kinds of semantics, i.e. the Shadow- (qualitative, possibilistic) and Hyperdistribution- (quantitative, probabilistic) structures we have built for noninterference with a refinement partial order (ie an implementation order that respects secrecy). Unusually, the two models will be described at the same time, interleaved; in this way I will try to bring out their similarities and differences.

If time permits, an example will be given of the kind of program algebra that results, and how the qualitative- and quantitative algebras can work together.

Talk B (noon): Roll-your-own notations for elementary probability

Abstract: Computer-science style reasoning about programs always benefits from notations that are consistent, are easy to calculate with, and that avoid where possible a dependence on auxiliary definitions that must be given in some surrounding narrative. We are more interested in dry, systematic prose than in the mathematical poetry of objects that enjoy properties, of facts that are easy to see, and of hences, therefores and so-thats.

Notations for elementary probability theory seem to respond especially to a formal-methods motivated reorganisation that recognises the essential role of free- and bound variables, of expressions standing in-line for functions and of step-by-step calculation--- at least when the probabilities are applied to program semantics.

In this talk I will present an alternative notation for elementary probability theory that is principally inspired by computer-science notations already in use elsewhere; and I will give examples of it that are based on well known probability puzzles.

The talk is stand-alone, and not at all complicated; but its purpose is not to help to solve puzzles. Rather the motivation for paying the cost of using an alternative notation is provided by THE OTHER talk (and other works), where it allows a much more succinct and reliable presentation of the essential ideas.

9th November 2011	**Speaker:** Cas Cremers (Swiss Federal Institute of Technology, Zurich) **Title:** Exchanging a key - How hard can it be? **Abstract:** Many current proposals for key exchange protocols are proven secure with respect to variants of the Bellare-Rogaway notion for secure key exchange. We revisit the evolution of Bellare-Rogaway style security notions for authenticated key exchange and the concept of the "strongest possible adversary". We highlight some of the open issues and propose a new model, called eCK-PFS, and a new notion of deniability. We propose a new key exchange protocol that satisfies our security model and deniability notion. (The talk is based on the material presented in the recent papers One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability and Examining indistinguishability-based security models for key exchange protocols, that appeared in ASIACCS '11).
3rd November 2011	**Speaker:** Keith Mayes (Smart Card Centre, ISG, RHUL) **Title:** From Smart Cards to NFC Smart Phones **Abstract:** Smart Cards have been evolving and changing from cards with contacts to contactless cards and RFIDs. The need for attack resistant hardware has remained and smart cards/RFIDs are targeted by very organised and growing hacker/enthusiast communities. The most significant recent development in the smart card/RFID world is the arrival of Near Field Communications (NFC) that allows NFC capable mobile phones to act as card/RFID readers or to actually emulate the cards/RFIDS. There is lots of excitement regarding new applications, but also many security concerns that have led to the definition in standards of Security Elements (SE). However there are several competing options that have left security holes and some modes of operation do not use the SE, but rely on proprietary code control mechanisms. Not only does this put the phone platforms and applications at risk, but hacker/enthusiasts see the NFC platform as a powerful attack tool for skimming and clone emulation! This also adds to worries about the general security of phone platforms arising from published attacks. The talk will provide a brief overview of the topic and link in with some practical research carried out in the ISG Smart Card Centre.

27th October 2011	**Speaker:** Dusko Pavlovic (ISG) **Title:** New directions in security by obscurity **Abstract:** Shannon sought security against the attacker with unlimited computational powers: *if an information source conveys some information, then Shannon's attacker will surely extract that information*. Diffie and Hellman refined Shannon's attacker model by taking into account the fact that the real attackers are computationally limited. This idea led to modern cryptography. Shannon also sought security against the attacker with unlimited logical and observational powers, expressed through the maxim that "the enemy knows the system". This view is still endorsed in cryptography. The popular formulation, going back to Kerckhoffs, is that "there is no security by obscurity", meaning that the algorithms cannot be kept obscured from the attacker, and that security should only rely upon the secret keys. In fact, modern cryptography goes even further than Shannon or Kerckhoffs in tacitly assuming that *if there is an algorithm that can break the system, then the attacker will surely find that algorithm*. The attacker is not viewed as an omnipotent computer any more, but he is still construed as an omnipotent programmer. The ongoing hackers' successes seem to justify this view. So the Diffie-Hellman step from unlimited to limited computational powers has not been extended into a step from unlimited to limited logical or programming powers. Is the assumption that all feasible algorithms will eventually be discovered and implemented really different from the assumption that everything that is computable will eventually be computed? I will present some explorations towards refining our views of the attacker, and of the defender, by taking into account their limited logical and programming powers. If the adaptive attacker actively queries the system to seek out its vulnerabilities, can the system gain some security by actively learning attacker's methods, and adapting to them? (This is ongoing work, closely related with the paper Gaming security by obscurity and to some extent also with the subsequent discussions on the web.)
20th October 2011	**Speaker:** Jason Crampton (ISG) **Title:** Practical constructions for the efficient cryptographic enforcement of interval-based access control policies **Abstract:** The enforcement of authorization policies using

	cryptography has received considerable attention in recent years. Such enforcement schemes vary in the amount of storage and the number of key derivation steps that are required in the worst case. These parameters correspond, respectively, to the number of edges and the diameter of the graph that is used to represent the authorization policy. In this talk we will consider a particular class of access control policies and the associated graphs. We then present a number of techniques for constructing a new graph that has a smaller diameter than the original graph but enforces the same authorization policy.
13th October 2011	**Speaker:** Geoffrey S. Smith (Florida International University, Miami, FL, USA) **Title:** Quantifying Information Flow Using Min-Entropy **Abstract:** One of the most fundamental issues in computer security is to prevent the leakage of secret information to public outputs. But while it is sometimes possible to stop such leakage completely, it is perhaps more typical that some leakage is unavoidable. For instance an ATM machine that rejects an incorrect PIN thereby reveals that the secret PIN differs from the one that was entered. More subtly, the amount of time taken by a cryptographic operation may reveal information about the secret key. Hence the last decade has seen growing interest in quantitative theories of information flow, to allow us to talk about "how much" information is leaked and (perhaps) allow us to tolerate "small" leaks. But while it is tempting to measure leakage using classic information-theoretic concepts like Shannon entropy and mutual information, these turn out not to provide very satisfactory security guarantees. As a result, several researchers have developed an alternative theory based on Rényi's min-entropy. In this theory, leakage is measured in terms of a secret's vulnerability to being guessed in one try by an adversary; note that this is the complement of the Bayes Risk. In this talk, we will describe the basic theory of min-entropy leakage in deterministic and probabilistic systems, including comparisons with mutual information leakage, results on min-capacity, and results on channels in cascade. We will also discuss algorithms for calculating leakage in systems, and mention some applications, such as bounds on timing attacks on cryptography.
6th October 2011	**Speaker:** Maximilien Gadouleau (Queen Mary, University of London, UK) **Title:** Combinatorial representations for secure data

	dissemination **Abstract:** Combinatorial representations can be used to solve a problem on information security, where we want to ensure that an adversary with partial access to the messages transmitted cannot decode the messages it intercepts. Suppose a source wishes to transmit a given number r of symbols to a collection of trusted receivers. The source may send r messages to each receiver, all of them functions of the original symbols. However, an adversary wishing to know all the r original symbols can intercept r transmitted messages (but cannot access all the messages sent to a given receiver). Can the source select how to encode the messages so that the adversary will never be able to decode its messages? This question is equivalent to the existence of a combinatorial representation. Combinatorial representations are generalisations of linear representations of matroids based on functions over an alphabet. In this talk, we define representations of a family of bases (r-sets of an n-set). We first show that any family is representable by matrices over some finite alphabet. We then give a characterisation of families representable over a given alphabet as subgraphs of a determined hypergraph. If time permits, we finally show how other concepts from matroid theory (rank function, closure operator etc.) can be used to characterise the representations. These results show how the problem above can be solved, and how much information the adversary will be able to infer.
29th September 2011	**Speaker:** Trent Jaeger (Penn State University, University Park, PA, USA) **Title:** Towards System-Wide, Deployment-Specific MAC Policy Generation for Proactive Integrity Mediation **Abstract:** Preventing attacks proactively in modern distributed systems is a major challenge. The addition of mandatory access control (MAC) enforcement in commodity software was supposed to prevent such attacks by limiting the number of processes accessible to adversaries and confining those still accessible. Unfortunately, the task of security professionals is still reactive, fixing vulnerabilities as adversaries identify them. We claim that in order to configure systems to defend themselves from attacks proactively, MAC enforcement must be customized to the target deployment. However, OS distributors currently focus on designing generic MAC policies for all their customers, leaving system administrators with the difficult task of composing and customizing these policies for their deployment manually. In this talk, we propose the Proactive Integrity Methodology, a mostly-automated method that computes system-wide MAC policies to prevent attacks

	proactively for distributed system deployments. We constructed a tool that implements this methodology to generate system-wide, Decentralized Information Flow Control (DIFC) MAC policies that require near-minimal effort to make an information flow safe system for Linux web application deployments in tens of seconds. System administrators can use such a tool to generate deployment-specific MAC policies for their distributed systems and verify whether OS distributions satisfy those policies, enabling proactive configuration to prevent attacks.
5th September 2011	**Speakers:** Jaap-Henk Hoepman (Radboud University, Nijmegen, The Netherlands) **Title:** Revoking self-blindable credentials **Abstract:** Self-blindable credentials have recently been proposed to implement anonymous credentials in smart card environments. To implement revocation in this setting is hard. In fact, we show that existing protocols based on self-blindable credentials that include revocation are broken. We present a new protocol, that includes revocation, and prove it secure. This shows that in principle revocation of self blindable credentials is possible, albeit for the moment with a non-negligible efficiency penalty. The Digital Security group of the Radboud University Nijmegen is the largest security and privacy research institute in the Netherlands. We are involved in many projects that involve smart cards, RFID, applied cryptography and the like on topics like smart metering and public transport ticketing. The talk will start with a brief overview of our work in these areas.
18 July 2011 (1pm)	**Speaker:** David Freeman (Stanford University, USA) **Title:** Homomorphic Signatures for Polynomial Functions **Abstract:** We describe a homomorphic signature scheme that is capable of evaluating multivariate polynomials on signed data. Given the public key and a signed data set, there is an efficient algorithm to produce a short signature that authenticates the mean, standard deviation, least-squares fit, and other functions of the signed data. Previous systems for computing on signed data could only handle linear operations. Our system uses ideal lattices in a way that is a "signature analogue" of Gentry's construction of fully homomorphic encryption. Security is based on hard problems on ideal lattices similar to those in Gentry's system. This is joint work with Dan Boneh and appeared at Eurocrypt 2011.
7th July 2011	**Speaker:** Doug Stinson (University of Waterloo) **Title:** A Unified Approach to Combinatorial Key Predistribution

	Schemes for Sensor Networks **Abstract:** There have been numerous recent proposals for key predistribution schemes for wireless sensor networks based on various types of combinatorial structures such as designs and codes. We provide a unified framework to study these kinds of schemes. We derive general formulas for the metrics of the resulting key predistribution schemes that can be evaluated for a particular scheme simply by substituting appropriate parameters of the underlying combinatorial structure. This is joint work with Maura Paterson.
30th June 2011	**Speaker:** Dusko Pavlovic (ISG, RHUL) **Title:** Diagrams for cryptography? **Abstract:** Cryptography is a theory of secret functions. Category theory is a theory of functions in general. Cryptographic proofs are often sequences of complicated formulas. Categorical proofs are sometimes just as bad; but sometimes they are simplified using various diagrammatic techniques. Could similar devices be useful in cryptography? Is there a categorical cryptography? I will present some preliminary explorations in this direction.
23rd June 2011	**Speaker:** Mark Manulis (TU Darmstadt, Germany) **Title:** Social Authentication with Privacy **Abstract:** The establishment of friendship and business ties, based on personal social proximity captures the essence of "social authentication" and belongs to the most recognized contact establishment principles within our society. By the "six degrees of separation" hypothesis, originated in late 20's and empirically confirmed by modern social networking communities (e.g. Facebook), any pair of individuals is connected by roughly six intermediate ties. The expansion of our social activities towards the Internet, in particular through the increasing use of mobile devices for social interactions, irrespective of time and space, offers a new dimension for social authentication, yet, it prompts a number of privacy concerns. Unprotected disclosure of personal social ties may lead to an unforeseen negative impact for all involved parties. Efficient solutions for their privacy-preserving discovery are most welcome, should the opportunities offered for social authentication in "social clouds" become usable without further risks. In this talk I will focus on the core problem for privacy-preserving social authentication: Two unfamiliar users wish to assess their social proximity by discovering their common social ties to other users. How can they do it without disclosing their unrelated ties? Our solution to this problem is Private Contact Discovery (PCD), a surprisingly efficient and provably secure cryptographic protocol that lets two users on input their respective contact lists, learn their common contacts (if any), and nothing else. The latter property is captured by the privacy requirement of "contact-hiding", which is introduced as part of the formal security model for PCD. The protocol prevents

	manipulations of contact lists by means of user-based certification for existing contacts and furthermore allows their revocability. The PCD protocol works irrespective of the underlying network topology (e.g. p2p or centralized), does not require any trusted third parties, and can be deployed on mobile devices. Experimental analysis attests to the practicality of the PCD protocol, which achieves computational and communication overhead (almost) linear in the number of direct contacts. During my talk I will briefly introduce several cryptographic building blocks (full domain hash RSA, Okamoto-Tanaka certified (identity-based) key exchange, index-hiding message encoding) to simplify the presentation of the PCD protocol and clarify its design. I will explain why existing approaches such as private set intersection or anonymous credentials, although being related, do not provide an appropriate solution to the PCD problem. The PCD protocol appeared in the Applied Cryptography and Network Security 2011 conference as part of the joint paper with Emiliano De Cristofaro (University of California, Irvine) and Bertram Poettering (TU Darmstadt/CASED).
16th June 2011	**Speaker:** Kenneth Radke (Information Security Institute, QUT, Australia) **Title:** Ceremony Analysis: Strengths and Weaknesses **Abstract:** We investigate known security flaws in the context of security ceremonies to gain an understanding of the ceremony analysis process. The term "security ceremonies" is used to describe a system of protocols (including out-of-band flows and initialisation) and humans which interact for a specific purpose. Security ceremonies and ceremony analysis is an area of research in its infancy though it is being considered in a range of security settings, including formal methods, applied cryptography and network security. To better understand the issues involved, we analyse three ceremonies previously shown flawed, HTTPS, EMV and Opera Mini, and use the information gained from the experience to establish a list of typical flaws in ceremonies. Finally, we use that list to analyse a protocol proven secure for human use. This leads to a realisation of the strengths and weaknesses of ceremony analysis.
9th June 2011	**No Seminar**
2nd June 2011	**No Seminar**
26th May 2011	**Speaker:** Angelo De Caro (University of Salerno, Italy) **Title:** Hidden Vector Encryption Fully Secure Against Unrestricted Queries **Abstract:** Predicate encryption is an important cryptographic primitive that enables fine-grained control on the decryption keys. Let P be a binary predicate. Roughly speaking, in a predicate encryption scheme for predicate P the owner of the master secret key can derive secret key, for any vector y. In

	encrypting a message M, the sender can specify an attribute vector x and the resulting ciphertext can be decrypted only by using keys, for vectors y, such that P(x,y)=1. Our main contribution is the first construction of a predicate encryption scheme that can be proved fully secure against unrestricted queries by probabilistic polynomial-time adversaries under non-interactive constant sized (that is, independent of the length L of the attribute vectors) hardness assumptions on bilinear groups of composite order. Specifically, we consider hidden vector encryption (HVE in short), a notable case of predicate encryption introduced by Boneh and Waters [TCC 2007]. In a HVE scheme, the ciphertext attributes are vectors x of length L over alphabet sigma, keys are associated with vectors y of length L over alphabet sigma with the special * symbol and we consider the Match(x,y) predicate which is true if and only if, for all i, y_i != * implies x_i=y_i. Previous constructions restricted the proof of security to adversaries that could ask only non-matching queries; that is, for challenge attribute vectors x_0 and x_1, the adversary could ask only for keys of vectors y such that Match(x_0,y)=Match(x_1,y)=0. Our proof employs the dual system methodology of Waters [Crypto 2009], that gave one of the first fully secure construction in this area, blended with a careful design of intermediate security games that keep into account the relationship between challenge ciphertexts and key queries.
23rd May 2011	**Speaker:** Hoeteck Wee (Queens College, CUNY - USA) **Title:** Threshold and Revocation Cryptosystems via Extractable Hash Proofs **Abstract:** We present a new unifying framework for constructing non-interactive threshold encryption and signature schemes, as well as broadcast encryption schemes, and in particular, derive several new cryptosystems based on hardness of factoring, including: (i) a threshold signature scheme (in the random oracle model) that supports ad-hoc groups (i.e., exponential number of identities and the set-up is independent of the total number of parties) and implements the standard Rabin signature; (ii) a threshold encryption scheme that supports ad-hoc groups, where encryption is the same as that in the Blum-Goldwasser cryptosystem and therefore more efficient than RSA-based implementations; (iii) a CCA-secure threshold encryption scheme in the random oracle model; (iv) a broadcast encryption scheme (more precisely, a revocation cryptosystem) that supports ad-hoc groups, whose complexity is comparable to that of the Naor-Pinkas scheme; moreover, we provide a variant of the

	construction that is CCA-secure in the random oracle model. Our framework rests on a new notion of threshold extractable hash proofs. The latter can be viewed as a generalization of extractable hash proofs, which are a special kind of non-interactive zero-knowledge proof of knowledge.
19th May 2011	**Speaker:** Ciaran Mullan (ISG, RHUL) **Title:** A view on group-based cryptography **Abstract:** Group-based cryptography has its origins in the mid 1980's. Since then there have been many cryptographic proposals based on group theoretic ideas, and almost as many breaks on these proposals. However, cryptanalysis has led to some new questions in group theory and beyond. In the first half of this talk we give an overview of the main ideas in group-based cryptography. In the second half we offer a cryptanalysis of a couple of key establishment protocols that employ certain matrix groups as a platform. In the third half we discuss some recent open problems in the area.
12th May 2011	**Speaker:** Imad Abbadi (Computing Laboratory, Oxford University - UK) **Title:** Toward Trustworthy Clouds' Internet Scale Critical Infrastructure **Abstract:** Cloud computing is a new concept using old technologies that have emerged from industry to academia. This result in some confusion about Cloud potential capabilities by overestimating some features and underestimating the challenges. We present an overview of Cloud critical infrastructure focusing on what is known as IaaS (Infrastructure as a Service) Cloud type. We then discuss security challenges and requirements, which would hopefully contribute in moving current Cloud untrusted infrastructure to a trustworthy Internet-scale Cloud critical infrastructure.
5th May 2011	**Speaker:** Frederik Armknecht (Universität Mannheim, Germany) **Title:** On Constructing Homomorphic Encryption Schemes from Coding Theory **Abstract:** In this talk, we investigate the construction of homomorphic encryption schemes where the security can be reduced to the hardness of decoding problem. We show that such schemes are indeed possible by presenting a natural construction principle. Interestingly, these possess several non-standard positive features. First, they are not restricted to linear homomorphism but allow for evaluating multivariate polynomials up to a fixed (but arbitrary) degree d on encrypted field elements. Second, they can be instantiated with various error correcting codes, even for codes with poor correcting capabilities. Third, depending on the deployed code, one can achieve very efficient schemes. As a concrete example, we

	present an instantiation based on Reed-Muller codes where for d=2 and 3 and security levels between 80 and 128 bits, all operations take less than a second (after some pre-computation). However, our analysis reveals also limitations on this approach. For structural reasons, such schemes cannot be public-key, allow for a limited number of encryptions only, and cannot be combined with the bootstrapping technique. We argue why such schemes are nonetheless useful in certain application scenarios and discuss future directions on how to overcome these issues.
28th April 2011	**No Seminar**
21st April 2011	**No Seminar**
14th April 2011	**Speaker:** Matt Robshaw (Orange Labs, France) **Title:** Lightweight Cryptography Revisited **Abstract:** Over recent years, there has been considerable activity in the field of "lightweight cryptography". In this seminar we review recent developments from both an academic and an industry perspective.
7th April 2011	**Speaker:** Cathy Meadows (Naval Research Laboratory - Washington, USA) **Title:** Deriving Ephemeral Authentication Using Channel Axioms **Abstract:** In recent years, the concept of a computer network has expanded greatly beyond the notion of a wired network whose nodes have permanent addresses. Communication channels include not only computer-to-computer channels implemented via cables, but wireless channels, human-to-computer and even human-to-human channels, and traditional cryptographic means of authentication are now supplemented via additional information such as biometrics, location information, and solutions to CAPTCHAS. In some cases, the information may be permanently to a node or individual, in others it may vary over time. In many cases, the properties of the communication channels used can be leveraged to assist in verification of these properties. For example, the round-trip time of a wireless challenge and response can be used to verify proximity. These methods require new means of reasoning about and specifying the properties the communication channels used in authentication, so that the guarantees provided by using these channels can be accounted for. In this talk we show how we are extending the Protocol Derivation Logic, a language originally designed for reasoning about cryptographic protocols, to reason about these new applications.
31st March 2011	**Speaker:** Andreas Pashalidis (KU Leuven, Belgium) **Title:** Relations among privacy notions **Abstract:** In this talk I will introduce a hierarchy of privacy

	notions, based on left-or-right indistinguishability. It will be shown how the definition relates to existing definitions from group signatures and anonymous communication systems. Moreover, the talk will present a novel way to measure unlinkability in a setting where the adversary may have access to arbitrary background information.
24th March 2011	**Speaker:** Martijn Stam (University of Bristol, UK) **Title:** Attacking the Knudsen-Preneel Compression Functions **Abstract:** Knudsen and Preneel (Asiacrypt'96 and Crypto'97) introduced a hash function design in which a linear error-correcting code is used to build a wide-pipe compression function from underlying blockciphers operating in Davies-Meyer mode. In this talk, we (re)analyse the security of the Knudsen-Preneel compression functions in the setting of public random functions. We give new non-adaptive preimage- and collision-finding attacks, that demonstrate that the original security claims are incorrect. We explain why an important tool in reducing the time complexity of our attacks is the dual code. [joint work with Onur Ozen and Thomas Shrimpton]
17th March 2011	**No Seminar**
10th March 2011	**Speaker:** Jacob Schuldt (RCIS - AIST, Japan) **Title:** On-line Non-transferable Signatures Revisited **Abstract:** Undeniable signatures, introduced by Chaum and van Antwerpen, and designated confirmer signatures, introduced by Chaum, allow a signer to control the verifiability of his signatures by requiring a verifier to interact with the signer to verify a signature. An important security requirement for these types of signature schemes is non-transferability which informally guarantees that even though a verifier has confirmed the validity of a signature by interacting with the signer, he cannot prove this knowledge to a third party. Recently Liskov and Micali pointed out that the commonly used notion of non-transferability only guarantees security against an off-line attacker which cannot influence the verifier while he interacts with the signer, and that almost all previous schemes relying on interactive protocols are vulnerable to on-line attacks. To address this, Liskov and Micali formalized on-line non-transferable signatures which are resistant to on-line attacks, and proposed a generic construction based on a standard signature scheme and an encryption scheme. In this talk, we revisit on-line non-transferable signatures. Firstly, we extend the security model of Liskov and Micali to cover not only the sign protocol, but also the confirm and disavow protocols executed by the confirmer. Our security model furthermore considers the use of multiple (potentially corrupted or malicious) confirmers, and guarantees security against attacks related to the use of signer specific confirmer keys. We then

	present a new approach to the construction of on-line non-transferable signatures, and propose a new concrete construction which is provably secure in the standard model. Unlike the construction by Liskov and Micali, our construction does not require the signer to issue "fake" signatures to maintain security, and allows the confirmer to both confirm and disavow signatures. Lastly, our construction provides noticeably shorter signatures than the construction by Liskov and Micali.
3rd March 2011	**Speaker:** Björn Tackmann (ETH Zurich, Switzerland) **Title:** Authenticate-then-Encrypt: A Constructive Perspective **Abstract:** Secure communication is often characterized by two basic properties: confidentiality and authenticity. To achieve these properties with symmetric cryptography, one would usually employ encryption schemes and MACs, respectively. Two such schemes can be composed in different ways, all of which are used in practical protocols: Encrypt-then-Authenticate (ESP), Authenticate-then-Encrypt (TLS), or Encrypt-and-Authenticate (SSH). Yet, it turns out that this composition is more subtle than one might initially expect, and there are, for example, several works questioning the security of AtE-based protocols. In contrast, AtE is known to be secure for certain combinations of schemes [Krawczyk, 2001]. In this talk, we analyze the AtE-paradigm from a different - constructive [Maurer, 2010] - perspective. That is, instead of modeling the security of the employed schemes by showing the impossibility of attacks, we explicitly formulate the guarantees provided to the users. This leads to a characterization of the malleability of encryption schemes, and indeed we show that the AtE-paradigm is sound for all schemes that exhibit a certain restricted type of malleability.
24th February 2011	**Speaker:** Valerio Genovese (University of Luxembourg and University of Torino) **Title:** Distributed Authorizations Policies: Modal Logic and Answer Set Programming **Abstract:** We discuss the theoretical and practical benefits in using modal logic and answer set programming (ASP) to specify, reason and enforce distributed access control policies. In the first part of the talk we introduce Modal Access Control Logic (M-ACL) which embeds the well-known "says" operator into a constructive modal logic. We then present ACL-Lean, an efficient Prolog implementation of M-ACL proof theory which outperforms state of the art tools to reason about access control. In the second part we present an approach for distributed access control policies that is based on a nonmonotonic semantics and the use of logic programming for policy specification and the evaluation of access requests. In particular we extend ASP to allow assertions of relevance to access control to be made by

	individual agents or on a community-based level and different strengths of testimonial warrant may be distinguished by using various logical operators. Moreover, we present a DLV-based implementation that allows for remote access request evaluation.
17th February 2011	**Speaker:** Wolter Pieters (University of Twente, Netherlands) **Title:** Humans and Information Security: E-Voting, the Cloud, and Actor-Networks **Abstract:** The abolition of the electronic voting machines in the Netherlands taught us some important lessons about information security. Firstly, the societal goals to be achieved with information security are still unclear, and privacy impact assessments are not sufficiently broad to assess all potential problems. Secondly, although there is a lot of concern about high-tech attacks, most things that we know to have gone wrong are low-tech approaches focusing on human weaknesses. These insights also shed new light on the current discussion on cloud computing and its (in)security. I have put forward two proposals to address these questions. The first, to be touched upon only briefly, is the translation of principles from environmental ethics to anchor information security in the policy domain. The second is a framework for including human actions in threat assessment of information systems, based on actor-network theory. I will explain the assumptions, formal model and threat assessment procedure derived from the application of this theory, and identify challenges for future research.
10th February 2011	**Speaker:** Martin Albrecht (LIP6 - UPMC, France) **Title:** PollyCracker Revisited **Abstract:** Since Gentry's seminal work on homomorphic encryption, this area has received considerable attention from the cryptographic community. Perhaps one of the most natural homomorphic schemes conceivable is PollyCracker which is naturally homomorphic. However, almost all PollyCracker inspired schemes that have been proposed so far have been badly broken. In fact, it was conjectured about 15 years ago in "Why you cannot even hope to use Gr√∂bner Bases in Public Key Cryptography: an open letter to a scientist who failed and a challenge to those who have not yet failed" that it was impossible to construct a secure PollyCracker-style scheme. In this work we initiate a formal treatment of cryptosystems based on the hardness of Gr√∂bner basis computations for random systems of equations, discuss their limitations, why standard techniques from homomorphic encryption research fail in this area, and propose a PollyCracker variant based on polynomial system solving with noise which is a first step towards a provably secure PollyCracker public-key scheme.
3rd February 2011	**Speaker:** Ludovic Perret (LIP6 - UPMC, France) **Title:** Improved Algebraic Cryptanalysis of McEliece Cryptosystem **Abstract:** The McEliece‚Äôs scheme relies on the use of error-

	correcting codes. A new algebraic approach to investigate the security of the McEliece has been proposed by Faug√®re-Otmani-Perret-Tillich (FOPT) at Eurocrypt 2010. It has been proved that the private key of the cryptosystem satisfies a system of bi-homogeneous polynomial equations. This property is due to the particular class of codes considered which are alternant codes. These highly structured algebraic equations allowed to mount a efficient key-recovery attack against two recent variants of the McEliece cryptosystems that aim at reducing public key sizes by using quasi-cyclic or quasi-dyadic structures. In the first part of the talk, we present an improved complexity analysis of this attack. Indeed, thanks to a very recent development due to Faug√®re-Safey el Din-Spaenlehauer on the solving of bihomogeneous bilinear systems, we can estimate the complexity of the FOPT algebraic attack. This is a first step toward providing a concrete criterion for evaluating the security of future compact McEliece variants. In the second part of the talk, we plan to study the difficulty of the Goppa Code Distinguishing (GD) problem, which is the problem of distinguishing the public matrix in McEliece's cryptosystem from a random matrix. It is widely believed that this problem is computationally hard as proved by the increasing number of papers using this hardness assumption. One can consider that disproving/mitigating this hardness assumption is a breakthrough in code-based cryptography. We present a efficient distinguisher for alternant and Goppa codes over binary/non binary fields. The distinguisher is based on the FOPT attack.
27th January 2011	**Speaker:** Allan Tomlinson (ISG, RHUL) **Title:** Privacy assessment of an enterprise social network **Abstract:** The Mobile VCE `Instant Knowledge' project aims to provide an autonomous social network within an enterprise environment. The aim is to connect members of the enterprise with colleagues who have relevant expertise, hence revealing new sources of information and resources. The project aims to make use of the context information to automatically update the user's social network, and make available to them knowledge about their contacts which would otherwise be hidden. As with any social network, privacy is a concern. More so when context data is gathered and distributed automatically. This talk will illustrate the privacy threats to this system by applying `mis-use' cases, and discuss the general implications and privacy requirements that can be derived from this exercise.
20th January 2011	**Speaker:** Andreas Peter (Technische Universitaet Darmstadt, Germany) **Title:** A Cleaner View on IND-CCA1 Secure Homomorphic Encryption using SOAP **Abstract:** Informally, a public-key encryption scheme is called homomorphic, if it allows one to evaluate certain functions over encrypted data without being able to decrypt. These schemes are

	being extensively studied as they provide the basis for various important applications, such as Outsourcing of Computation, Electronic Voting, Private Information Retrieval, etc. In this talk, I will give a complete characterization both in terms of security and design of a large class of such schemes that particularly comprises the prominent examples ElGamal and Paillier. This is done by considering the security and structure of a certain abstract scheme that represents the whole class. For instance, one can show that its IND-CCA1 security is equivalent to the hardness of a new abstract problem called Splitting Oracle-Assisted Subgroup Membership Problem (SOAP). To highlight the significance of this result, I will then explain its use for determining the security of existing schemes, deriving impossibility results, and constructing new schemes. [This is joint work with Frederik Armknecht and Stefan Katzenbeisser]
13th January 2011	**Speaker:** Tomohiro Sekino (Chuo University - Japan) **Title:** Privacy Enhanced Radio Frequency Identification **Abstract:** One application of RFID systems is entering and leaving management systems of a room using RFID systems. In such systems, the management system checks if a person has a permission to enter the room. However, since in usual RFID systems the ID of a tag is sent via radio waves, anyone can easily eavesdrops some information between the reader and the tag. One's location could be traced from the eavesdropped information. Therefore, information between the reader and the tag should be send confidentially. If we use a symmetric key encryption scheme, the receiver must search a corresponding key and this needs heavy computational cost, if many people have registered to this system. Thus, public key encryption scheme is suitable for this purpose. However it is difficult to implement public key encryption on RFID due to the heavy computational cost. To solve this problem, we use Niederreiter PKC whose encryption process is lighter than other PKE schemes such as RSA, ElGamal and so on. However, encryption key size of Niederreiter PKC is too large, that is about 2M bits. In our study, we succeed to reduce encryption key size of Niederreiter PKC. We apply construction of code and devise encryption processing. Finally, we show that encryption key size can be reduced to 5,000 bits. If our study become reality, RFID systems can securely authenticate without any exhaustive search in database.

Thursday 16th December 2010:
Speaker: Colin Boyd (Queensland University of Technology - Australia)

Title: DoS-resistant key exchange: models and mechanisms
Abstract: Security models for key exchange have been around for many years, but only recently have started to include consideration of denial-of-service attacks. This talk will consider security models for client puzzles and in particular introduce a new model to be presented at CT-RSA 2011. The new model incorporates the possibility that an adversary may attack multiple puzzles simultaneously. In addition we will consider the notion of gradual authentication as applied to key exchange and introduce a new mechanism combining client puzzles and digital signatures with fast verification.
This is joint work with Juan Gonzalez, Lakshmi Kuppusamy, Jothi Rangasamy and Douglas Stebila.

Thursday 9th December 2010:
Speaker: Lizzie Coles-Kemp (ISG, RHUL)
Title: Talking Privacy: Theory Building and Technology Design
Abstract: This talk presents work from the privacy research project Visualisation and Other Methods of Expression (VOME). The goal of this project is to develop social and digital technologies to support the selection of effective on-line privacy protection practices. In order to achieve this the project uses social research to build theories about the selection and use of on-line privacy protection practices and participatory design to develop the supporting technologies. This talk will focus on the theories emerging from the social research and sketch the resulting technology designs.

Extra Seminar to be held on TUESDAY at 11AM, in McCrea room 229
Tuesday 7th December 2010:
Speaker: Danny De Cock (KU Leuven, Belgium)
Title: Electronic Voting in Belgium - past and future
Abstract: This presentation gives an overview of the evolution process of the system used for electronic voting in Belgium since 1991, together with the rationale behind this evolution process. It also introduces the improved paper-based voting system that does use cryptography and that will replace the old system for elections after 2011.

Thursday 25th November 2010:
Speaker: Kenny Paterson (ISG, RHUL)
Title: The evolution of the SSL/TLS Record Protocol
Abstract: The SSL/TLS Record Protocol is the component of the SSL/TLS protocol suite that is responsible for providing confidentiality and integrity services to application data. In this talk, I will discuss how the SSL/TLS Record Protocol has evolved over time in response to various attacks and demands for greater functionality. I will then present a new attack against the cryptographic construction used by the current version of SSL/TLS.

Thursday 18th November 2010:
Speaker: Robert Granger (DCU, Ireland)
Title: On the Static Diffie-Hellman Problem on Elliptic Curves over Extension Fields
Abstract: Recent work by Koblitz and Menezes has highlighted the existence, in some cases, of apparent separations between the hardness of breaking discrete logarithms in a particular group, and the hardness of solving in that group problems to which the security of certain cryptosystems are provably related. We consider one such problem in the context of elliptic curves over extension fields, and report potential weaknesses of the Galbraith-Lin-Scott curves from EUROCRYPT 2009, as well as two very different practical attacks on the Oakley Key Determination Protocol curves.

Thursday 11th November 2010:
Speaker: Christian W Probst (Technical University of Denmark)
Title: Tackling insider threats: a definition, a formal model, and their limitations
Abstract: Insider threats are easy to counter. All we need is a concise model of human behavior and its dependencies on outer and inner influences, a surveillance system in place that is able to observe in necessary detail action and influences, and an evaluation system that can draw the necessary conclusions from its input. Neither of the components just described is easy to realise, or desirable to have in the first place. Modelling human behaviour is close to impossible, let alone modelling how it depends on outer and inner factors. A surveillance system is heavily dependent on legal boundaries of what is allowed to be monitored or not, and the amount of data even from legal monitoring can be overwhelming at best. An evaluation system would need to be able to take all the input and models into account, and this is yet another complex task.

In this talk we investigate the notion of insiders and insider threats from different viewpoints. From an organizational viewpoint, we derive a definition of how insiders can be characterized. We then develop a theoretical, modular system model that is expressive enough to model real world scenarios, yet simple enough to lend itself for extensions and integration with other techniques. The formal basis enables the development of different analysis techniques to identify possible insider attacks. Finally, we discuss a special extension, namely human behavior, and discuss how it can be added to the model. The talk concludes by investigating the plausibility of the term "insider".

Thursday 04th November 2010:
Speaker: Michael Tunstall (University of Bristol, UK)
Title: Distinguishing Multiplications from Squaring Operations and the Noisy Discrete Logarithm Problem
Abstract: We present experimental results in analysing the output of the word-by-word multiplication instructions on a common embedded processor (the ARM7), based on the difference in the distribution of the expected Hamming weight for multiplications and squaring operations. This allows us to obtain partial side channel information on the higher level operations performed by a public key operation using only one execution. This partial information is then refined further using a modification of previous methods based on Hidden Markov Models, resulting in a new computational problem which we call the Noisy Discrete Logarithm Problem. For the latter problem we present a heuristic algorithm which seems to work well in practice. We stress our work is focused on the case were the attacker obtains side channel information for only one execution with respect to a given secret key, as one would have when attacking secret ephemeral exponents in discrete logarithm based systems. [Note: the seminar will concentrate on the practical side of this work and only touch on the noisy discrete logarithm problem]

Thursday 28th October 2010:
Speaker: Stephen D. Wolthusen (ISG, RHUL)
Title: Measuring Security Attributes in Partially Trusted Concurrent Environments
Abstract: We assume that security controls may fail and that a given system may be compromised, including the security controls themselves and particularly audit mechanisms or sensors. To determine the system security state it is, however, necessary to rely on such data sources and control mechanism.

In this talk we will discuss models for detecting (malicious) operations in concurrent, partially trusted environments under explicit, partially trusted communication channel constraints. We describe the simple case of a forced n-way synchronisation with probabilistic ordering, and also introduce the notion of cost models for synchronisation and observations. We also introduce the notion of communication channel constraints for adversaries and motivate this using an example from the control systems domain.

Thursday 21st October 2010:
Speaker: Mark Manulis (TU Darmstadt, Germany)
Title: Affiliation-Hiding Authentication
Abstract: In traditional PKI-based scenarios authentication is usually performed via digital signatures that, however, may leak information about the identity/public key of the signer. One way to hide the identity of an authenticating user is to resort to "group authentication" techniques. This privacy-preserving form of authentication, which is achievable with standard group signatures, may still be insufficient, when users wish to keep their group memberships (affiliations) private as well. This problem has been addressed by a relatively new research area of "secret handshakes" or "affiliation-hiding" authentication protocols, which are interactive cryptographic protocols allowing two or more users, being members of one or several groups, to authenticate each other, and possibly compute a secure communication key, in a way that preserves privacy of their identities and groups. In this talk I will present new solutions for obtaining stronger privacy guarantees in affiliation-hiding protocols and for improving the efficiency of such protocols in the (practice-relevant) multi-affiliation setting. (The talk is based on recent papers with Benny Pinkas, Bertram Poettering, and Gene Tsudik).

Thursday 14th October 2010:
Speaker: Jean Paul Degabriele (ISG, RHUL)
Title: On the (In)Security of IPsec in MAC-then-Encrypt Configurations
Abstract: IPsec allows a huge amount of flexibility in the ways in which its component cryptographic mechanisms can be combined to build a secure communications service. This may be good for supporting different security requirements but is potentially bad for security. In this talk we will demonstrate the reality of this by describing efficient, plaintext-recovering attacks against all configurations of IPsec in which integrity protection is applied prior to encryption ‚Äì so-called MAC-then-encrypt configurations. We report on the implementation of our attacks against a specific IPsec implementation, and reflect on the implications of our attacks for real-world IPsec deployments as well as for theoretical cryptography.
(talk presented at CCS 2010)

Thursday 07th October 2010:
Speaker: Alex Dent (ISG, RHUL)
Title: Broadcast encryption with multiple trust authorities
Abstract: Broadcast encryption allows a confidential message to be sent to a large group of people more efficiently than sending each an encrypted message individually. For sending information in highly-structured environments, one solution to the broadcast encryption problem is to use WIBEs (wildcarded identity-based encryption). However, WIBE systems have a single root of trust, which makes their use undesirable in situations where no single entity can be acknowledged as trusted by all parties in the system.

In this talk, we'll discuss the advantages and disadvantages of using WIBEs, then introduce the concept of a multiple-trust-authority WIBE. This allows highly-structured organisations

to form coalitions that allow encrypted messages to be broadcast to all parties inside the coalition without requiring a single root of trust. These coalitions can be temporary and dynamic in the sense that they can easily be established across public channels and that membership to one coalition does not allow any party to read messages sent to members of another coalition. We'll discuss the advantages and disadvantages of using this approach and give an example implementation.
(this talk was presented at LatinCrypt 2010)

Thursday 30th September 2010:
Speaker: Christine M O'Keefe (CSIRO - Australian Commonwealth Scientific and Research Organization)
Title: Remote Access for Privacy and Confidentiality Protection
Abstract: In a remote access system, users receive output from submitted statistical queries but do not have direct access to data. A remote access system may involve confidentialisation of the data itself or the system outputs, or both. In this talk I will give an introduction to remote access systems and discuss current international implementations. I will also use the CSIRO demonstrator "Privacy-Preserving Analytics" remote access system to give some concrete examples.

The programme for the 2009/2010 academic year was as follows:

Thursday 1st October 2009:
Speaker: Po Yau (ISG, RHUL)
Title: Enhancing Workflow Security using Trusted Computing and Virtualisation
Abstract: Information workflows can involve outsourcing segments to third parties. This is increasingly becoming common because of work into integration technologies, such as Web services, and the emergence of various forms of distributed computing, such as Grid computing and Cloud computing. We use Grid workflows, a set of tasks arranged into a logical order to process a Grid user's dataset, as an example for workflow security requirements addressing the needs of the Grid user. An overview of a secure protocol using Trusted Computing technology will be presented, which is further enhanced with platform virtualisation hardware and software. The proposed scheme allows the selection of trustworthy third parties and gives confidentiality and integrity protection to the workflow, the Grid user's processes and data. The scheme also detects any problems during workflow execution, collecting information that can be potentially used for process provenance.

Thursday 8th October 2009:
Speaker: Jason Crampton (ISG, RHUL)
Title: Trade-Offs in Key Assignment Schemes for Hierarchical and Temporal Access Control
Abstract: A key assignment scheme provides a framework for implementing hierarchical access control policies using encryption. We define several generic key assignment schemes and compare their respective advantages by considering the amount of public storage used and the number of steps required to derive a key. We then examine the specific trade-offs that exist for a particular type of key assignment scheme that has been used to implement temporal access control policies.

Thursday 15th October 2009:
Speaker: Liang Chen (ISG, RHUL)
Title: Set Covering Problems in Role-Based Access Control

Abstract: Interest in role-based access control has generated considerable research activity in recent years. A number of interesting problems related to the well known set cover problem have come to light as a result of this activity. However, the computational complexity of some of these problems is still not known. We explore some variations on the set cover problem and use these variations to establish the computational complexity of these problems. Most significantly, we prove that the minimal cover problem -- a generalization of the set cover problem -- is NP-hard, which is used to determine the complexity of the inter-domain role mapping problem. We also design a number of approximation algorithms for the minimal cover problem, and conduct some experiments to evaluate the quality of those algorithms. Joint work with Jason Crampton.

Thursday 22nd October 2009:
Speaker: Michael Huth (Imperial)
Title: Access Control via Belnap Logic: Intuitive, Expressive, and Analyzable Policy Composition
Abstract: Access control to IT systems is increasingly relying on the composition of policies - accelerated by the need to federate, self-configure or contextualize potentially heterogeneous systems. There is thus benefit in any framework that supports intuitive yet formal (and so ``analyzable'' and ``implementable'') policy compositions, abstracts away irrelevant aspects of application domains, provides a rich and efficiently analyzable set of non-adhoc compositions, and can realize generic and domain-specific extensions of its composition language on top of the framework core.

We here develop such a framework based on Belnap logic: an access-control policy is interpreted as a *four-valued* predicate that maps access requests to either Grant, Deny, Conflict, or Unspecified -- corresponding to the four-valued Belnap bilattice. Our core composition language contains the constant policy Unspecified, base policies that lift specifications of request sets to conflict-free policies, and operators for negation, conjunction, and implication in the truth ordering of the bilattice. These operators are obtained as pointwise extensions of the familiar operators on the Belnap bilattice. In this core language, important and convenient composition operator are derived, which enable the decoupling of conflict resolution from policy composition. We propose a query language for policy refinement checks, show that it can express important analyses (e.g. conflict analysis), and reduce query validity checking to validity checking of propositional logic. Finally, we evaluate our approach through the specification and analysis of firewall policies and RBAC policies and discuss domain-specific and generic extensions of our policy language.

Thursday 29th October 2009:
Speaker: Steve Williams (Bristol)
Title: Secure Two-Party Computation is Practical
Abstract: Secure multi-party computation has been considered by the cryptographic community for a number of years. Until recently it has been a purely theoretical area, with few implementations with which to test various ideas. This has led to a number of optimisations being proposed which are quite restricted in their application. In this paper we describe an implementation of the two-party case, using Yao's garbled circuits, and present various algorithmic protocol improvements. These optimisations are analysed both theoretically and empirically, using experiments of various adversarial situations. Our experimental data is provided for reasonably large circuits, including one which performs an AES encryption, a problem which we discuss in the context of various possible applications. Joint work with B. Pinkas, T. Schneider and N.P. Smart

Thursday 5th November 2009:
Speaker: Georg Fuchsbauer (ENS, Paris)
Title: Efficient Anonymous Proxy Signatures
Abstract: Consider a set of users each holding a secret signing key and publishing a verification key for digital signatures. "Anonymous proxy signatures" enable a user (delegator) to delegate her signing rights to any other user. The latter can then sign on behalf of the delegator while remaining anonymous. Moreover, received rights can be re-delegated; e.g., Alice delegates to Bob who in turn re-delegates to Carol. Carol can then create a proxy signature that is verifiable under Alice's public key and that does not reveal the identities of Bob and Carol. As for group signatures, in case of misuse, an authority can open signatures to reveal the chain of delegations and the signer's identity. Anonymous proxy signatures are a generalisation of both proxy signatures and dynamic group signatures. In order to efficiently instantiate the primitive using the non-interactive witness-indistinguishable proof system by Groth and Sahai (Eurocrypt 2008), we introduce "automorphic signatures" and give an efficient instantiation. A signature scheme in a bilinear group is automorphic if its verification keys lie in the message space, messages and signatures consist of group elements only, and verification amounts to evaluating a set of pairing-product equations. These signatures make a perfect counterpart to Groth-Sahai proofs and turn out to have many more applications.

Thursday 12th November 2009:
Speaker: Cas Cremers (ETH Zurich)
Title: Formalizing and analyzing compromising adversaries
Abstract: We formalize a hierarchy of adversary models for security protocol analysis, ranging from a Dolev-Yao style adversary to more powerful adversaries who can reveal different parts of principals' states during protocol execution. We define our hierarchy by a modular operational semantics describing adversarial capabilities. We use this to formalize various, practically-relevant notions of key and state compromise. Our semantics can be used as a basis for protocol analysis tools. As an example, we extend an existing symbolic protocol-verification tool with our adversary models. The result is the first tool that systematically supports notions such as weak perfect forward secrecy, key compromise impersonation, and adversaries capable of so-called strong corruptions and state-reveal queries. As further applications, we use our model hierarchy to relate different adversarial notions, gaining new insights on their relative strengths, and we use our tool to find new attacks on protocols. Joint work with David Basin.

Thursday 19th November 2009:
Speaker: Christian Cachin (IBM Zurich)
Title: Cryptographic Interfaces: From Hardware-Security Modules to Open Key-Management Systems
Abstract: Cryptographic keys must be stored and managed. In real-world applications, they are often guarded by hardware-security modules (HSMs) with sophisticated physical protection. Several logical attacks through the key-management operations in cryptographic interfaces of HSMs have been reported in the past, which allowed to expose keys merely by exploiting the interface in unexpected ways. We are currently building a key-lifecycle management system accessible through an open protocol. We describe how to secure the system against attacks through its cryptographic interface. Its key-management operations integrate traditional access control with the semantics of cryptographic operations so that they respect the dependencies introduced through the cryptographic operations on keys. Based on

joint work with Mathias Björkqvist, Nishanth Chandran, Robert Haas, Xiao-Yu Hu, Anil Kurmus, René Pawlitzek, and Marko Vukolic.

Thursday 26th November 2009:
Speaker: Kostas Markantonakis (ISG, RHUL)
Title: Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems
Abstract: In this work we propose a mutual authentication protocol for RFID (Radio Frequency Identification) systems incorporating low-cost RFID tags. These tags, due to their limited computational capabilities do not incorporate advanced cryptographic primitives. As a result, there are various threats against users' privacy and against the security of such systems. Our protocol, PMM, utilizes a hash function and a pseudorandom number generator that can be hardware implemented in a low-cost RFID tag. The protocol offers a relatively high level of security by preventing replay attacks, Denial-of-Service attacks, tracking attacks, tag spoofing along with forward security and an enhanced protection of user privacy.

Thursday 3rd December 2009:
Speaker: Charles Morisset (ISG, RHUL)
Title: Comparing Access Control Models
Abstract: Many access control models exist in the literature and choosing one to enforce a security problematics require some tools both to implement it and to compare it with the others. We present here a formal generic definition of an access control model, based on the notion of state-machine, illustrated with well-known models (e.g. BLP or RBAC). We also define a preorder over access control models, mostly based on simulations, and compare formally some models, hence establishing a hierarchy among them. Indeed, we show that the Chinese Wall is strictly more restrictive than Bell & La Padula, which is strictly more restrictive than RBAC, which is equivalent to HRU. Joint work with Mathieu Jaume and Lionel Habib (LIP6)

Thursday 21st January 2010:
Speaker: Manuel Bernardo Barbosa (Universidade do Minho - Portugal)
Title: Deductive Verification of Cryptographic Software
Abstract: We apply state-of-the art deductive verification tools to check security-relevant properties of cryptographic software, including safety, absence of error propagation, and correctness with respect to reference implementations. We also develop techniques to help us in our task, focusing on methods oriented towards increased levels of automation, in scenarios where there are clear obvious limits to such automation. These techniques allow us to integrate automatic proof tools with an interactive proof assistant, where the latter is used off-line to prove once-and-for-all fundamental lemmas about properties of programs. The techniques developed have independent interest for practical deductive verification in general.

Thursday 28th January 2010:
Speaker: Carlos Cid (ISG, RHUL)
Title: Nonlinear Equivalence of Stream Ciphers
Abstract: We investigate (nonlinear) equivalences of LFSR-based stream ciphers using basic properties of Galois fields and certain nonlinear isomorphism maps. By doing this, we attempt to combine the analysis of both the sequence generator and the corresponding Boolean function in the security evaluation of filter generators. Our method can be seen as a way of constructing isomorphic ciphers and the focal point is then to study variance of cryptographic properties with respect to such an equivalence. It is shown that important

cryptographic properties used to evaluate the security of filter generators, such as non-linearity and algebraic immunity, are not invariant with respect to such an equivalence. We conclude that cryptanalysis in terms of isolating cipher-components is not sufficient, as a certain cryptographic measurement must hold for all isomorphic ciphers in a class. As a result, analysis of such properties are likely to be very difficult in practice when taking the class of isomorphic ciphers into account.
(joint work with Sondre Roenjom; to be presented at FSE 2010)

Thursday 4th February 2010:
Speaker: Pooya Farshim (ISG, RHUL)
Title: Strong Security Models for Public-Key Encryption Schemes
Abstract: In this talk, we first establish a connection between two strong variants of standard security notions for public-key encryption schemes: indistinguishability under strong chosen-ciphertext attacks and complete non-malleability. Strong chosen-ciphertext attacks model adversaries who can maliciously replace public keys of users and subsequently ask for decryptions under unknown secret keys. Completely non-malleable schemes on the other hand resist attacks which allow an adversary to tamper with both ciphertexts and public keys (which can be used in constructing non-malleable commitment schemes). We give the first precise definition of a strong decryption oracle, pointing out the subtleties in alternative approaches that can be taken. In particular, we specify how to deal with invalid ciphertext and/or public keys and the inherent ambiguity in the message that the oracle should return. We extend indistinguishability of ciphertexts, comparison-based non-malleability and simulation non-malleability under various attack models to allow strong decryption queries. We show that the known relations for the standard versions of these definitions naturally extend to their stronger versions. We end the first part by presenting a practical scheme, which is fully secure against strong chosen-ciphertext attacks, and therefore completely non-malleable, without random oracles.

In the second part of the talk, we introduce two extractor-based properties that allow us to gain insight into the design of completely non-malleable schemes and to go beyond known feasibility results in this area. We formalise strong plaintext awareness and secret key awareness and prove their suitability in realising these goals. Strong plaintext awareness imposes that it is infeasible to construct a ciphertext under any public key without knowing the underlying message. Secret key awareness requires it to be infeasible to output a new public key without knowing a corresponding secret key. We study the relations among these and existing notions in the literature and show that if such properties are realisable (and one admits non-black-box simulators) then the impossibility result established for the construction of completely non-malleable schemes under non-assisted simulators no longer holds. We also look at how such notions can be realised in the standard model and in the random oracle model. More precisely, we propose a generic transformation to construct secret key aware schemes in the random oracle model and give preliminary steps towards building such schemes in the standard model. To this end, we employ a technique used in designing escrow encryption schemes and introduce a new factorisation-based knowledge assumption.

Thursday 11th February 2010:
Speaker: Jan-Erik Ekberg (Nokia Research Center, Finland)
Title: The Mobile Trusted Module
Abstract: The Mobile Trusted Module (MTM) is a specification by the Trusted Computing Group that defines a common API and a set of functionality for embedded devices among

other things in the domains of secure boot, secure storage and attestation. It also defines an architecture by which this functionality can be mapped to legacy (processor) security architectures. The talk will briefly outline the use cases for, as well as the features of MTM, and as a case study outline a system adaptation done at the Nokia Research Center.

Thursday 18th February 2010 (This is a joint ISG/pure maths seminar)
Speaker: Mohan Shrikhande (Central Michigan University)
Title: A survey of embedding problems of Quasi-Residual Designs
Abstract: The notion of residual and derived design of a symmetric design goes back to a classic paper of R.C. Bose (1939). A residual design of a symmetric design D is a 2-design obtained from D by removing a block B and replacing every other block A by A\ B. A quasi-residual design is a 2-design which has the parameters of a residual design. A quasi-residual design which is a residual design is called embeddable.
In this survey talk, we begin with some classical results, then discuss some techniques for constructing quasi-residual designs and some different types of non-embeddability conditions. We include some recent results for families of non-embeddable quasi-residual designs. Proofs are provided for some new results and we give some tables of possible parameter sets of non-embeddable quasi-residual designs. This is joint work with T.A. Alraqad (see https://www.ma.rhul.ac.uk/pure_maths_seminars for more information).

Thursday 25th February 2010:
Speaker: Dave Boyd (ISG, RHUL)
Title: E-payments: Cardholder Privacy and Non-Repudiation
Abstract: Card payments tend not to keep the cardholder's details private, which can facilitate fraud, and it can be exceedingly difficult for a cardholder to repudiate a completed payment. This seminar is to outline proposed mechanisms to support cardholders by enhancing their privacy and non-repudiation capabilities.

Mechanisms are proposed that provide enhanced privacy and non-repudiation security services for both card-present and card-not-present payments. Each of these four categories of payment and security service requires its own scheme. Privacy is enhanced by stripping out personally identifiable information and using a different account number for each transaction. Non-repudiation is enhanced by leaving an electronic footprint after each transaction.

Web payments require particular attention. Banks are adept at authenticating clients. The final part of the seminar outlines further proposals to bring together those factors for a single sign-on service to the Web and a mechanism for client authentication in the TLS communications protocol.

Thursday 4th March 2010:
Speaker: Alex W. Dent (ISG, RHUL)
Title: Sufficient Conditions for Intractability over Black-Box Groups: Generic Lower Bounds for Generalized DL and DH Problems
Abstract: The generic (aka. black-box) group model is a valuable methodology for analyzing the computational hardness of number-theoretic problems used in cryptography. Since the properties ensuring generic hardness have not been well-studied and formalized yet, for each newly proposed problem an entire hardness proof has to be done from scratch.

In this work we identify criteria that guarantee the hardness of generalized DL and DH problems in an extended generic group model where algorithms are allowed to perform any operation representable by a polynomial function. Assuming our conditions are satisfied, we are able to provide negligible upper bounds on the success probability of such algorithms. As useful means for the formalization of definitions and conditions we explicitly relate the concepts of generic algorithms and straight-line programs that have only been used independently in cryptography so far.

Friday 12th March 2010 (note change of day/time for this week: the seminar will be on FRIDAY at 2PM, in room 229)
Speaker: Vitaly Shmatikov (The University of Texas at Austin, USA)
Title: New Directions in Privacy-Preserving Data Analysis
Abstract: The new Web economy relies on the collection of personal data on an ever-increasing scale. Information about our tastes, purchases, searches, browsing history, friendships and relationships, health history, genetics, and so forth is shared with advertisers, marketers, and researchers. The aggregated datasets do not exist in isolation; they contain implicit or explicit references to other datasets. Unsurprisingly, this raises a number of interesting privacy issues.

I will discuss the subtle relationship between anonymity and privacy, explain several techniques for de-anonymizing large datasets, and present experimental results which demonstrate how re-identification can be carried out on real-world datasets and social networks.

In the second part of the talk, I will describe the ongoing research on Airavat, a system for large-scale, privacy-preserving computation. Airavat is based on the MapReduce framework and includes a novel integration of mandatory access control and differential privacy. It enables users without security or privacy expertise to carry out computations on sensitive data, while ensuring compliance with the data providers' security policies.

Thursday 18th March 2010:
Speaker: Ludovic Perret (LIP6-UPMC Univ Paris 6 & INRIA, France)
Title: Algebraic Cryptanalysis of McEliece Variants with Compact Keys
Abstract: In this talk, we will present a new approach to investigate the security of the McEliece cryptosystem. We recall that this cryptosystem relies on the use of error-correcting codes. Since its invention thirty years ago, no efficient attack had been devised that managed to recover the private key. We prove that the private key of the cryptosystem satisfies a system of bi-homogeneous polynomial equations. This property is due to the particular class of codes considered which are alternanting codes. We have used these highly structured algebraic equations to mount an efficient key-recovery attack against two recent variants of the McEliece cryptosystems that aim at reducing public key sizes. These two compact variants of McEliece managed to propose keys with less than 20,000 bits. To do so, they proposed to use quasi-cyclic or dyadic structures. An implementation of our algebraic attack in the computer algebra system Magma allows to find the secret-key in a negligible time (less than one second) for almost all the proposed challenges. For instance, a private key designed for a 256-bit security has been found in 0.06 seconds with about 2^17.8 operations.
(joint work with Jean-Charles Faugere, Ayoub Otmani, and Jean-Pierre Tillich)

Friday 19th March 2010 (special seminar on FRIDAY at 2:30PM, in room 229)
Speaker: Chee Yeow Meng (Nanyang Technological University, Singapore)

Title: Universal Cycles, 2-Radius Sequences, and Fetching Huge Objects into Small Memory
Abstract: A new ordering, extending the notion of universal cycles, is proposed for the blocks of k-uniform set systems. Existence of minimum coverings of pairs by triples that possess such an ordering is established for all orders. This gives rise to 2-radius sequences that are shorter than those currently known, for all orders less than 10^36. Such sequences have application in cache algorithms.

Thursday 25th March 2010:
Speaker: Jon Hart (ISG, RHUL)
Title: Website Credential Storage and Two-factor Web Authentication with a Java SIM
Abstract: In this talk, two mobile authentication schemes are proposed. The first enables authentication credentials (username and password) to be stored and retrieved securely from a mobile handset and requires no changes to existing websites. The second scheme, which may optionally be used with the first, utilises a one-time password and is intended for applications requiring an enhanced level of authentication. Both authentication schemes use a Java SIM for secure storage of credentials and secret keys and the ubiquitous mobile phone; with its familiar and convenient form factor and high user acceptance.

There was no seminar on the 1st April, 8th April and 15th April 2010

Thursday 22nd April 2010:
Speaker: Robert Craven (Imperial College, UK)
Title: A Logic-Based Policy Analysis Framework with Dynamic System Component
Abstract: Despite several studies devoted to the analysis of policy-based systems, there is still no effective approach which answers all desiderata. Policy analysis ought to (i) be expressive, (ii) embrace both authorizations, positive and negative, and obligations, (iii) include a dynamic system model that can be involved in the analysis, and (iv) give useful diagnostic information in response to analysis queries. I will talk about a policy analysis framework, logic-based, which we have developed at Imperial in collaboration with IBM TJ Watson, which satisfies the above requirements. It allows the analysis of many significant policy-related properties, and has an associated implementation.

Thursday 29th April 2010:
Speaker: Maura Paterson (Birkbeck, Univ. of London)
Title: Error Decodable Secret Sharing and One-Round Perfectly Secure Message Transmission for General Adversary Structures
Abstract: An error decodable secret-sharing scheme is a secret-sharing scheme with the additional property that the secret can be recovered from the set of all shares, even after a coalition of participants corrupts the shares they possess. In this talk we will consider schemes that can tolerate corruption by sets of participants belonging to a monotone coalition structure, which generalise both a related notion studied by Kurosawa, and the well-known error-correction properties of threshold schemes based on Reed-Solomon codes. In addition, we will explore the connection between one-round perfectly secure message transmission (PSMT) schemes with general adversary structures and secret-sharing schemes, and we will exploit this connection to investigate factors affecting the performance of one-round PSMT schemes.

Thursday 6th May 2010:
Speaker: Simon Blackburn (ISG, RHUL)
Title: Cryptosystems based on group theory

Abstract: There have been regular proposals to use group theory to construct cryptographic primitives over the past decade. This talk will give a introduction to some of the ideas involved, and will describe and then cryptanalyse a recent scheme.

Thursday 13th May 2010:
Speaker: Gerhard Hancke (ISG, RHUL)
Title: RFID Security: A Guide to Practical Threats
Abstract: Privacy and security concerns regarding RFID have been extensively covered in technical publications, and several government institutions have formulated security guidelines for RFID. However, simply knowing about theoretical threat scenarios does not answer all the questions that users and operators continue to ask about RFID security. For example, intuitively most people would recognise that an RF channel could be eavesdropped but for them to accurately assess the risk it is important to know how practically feasible this attack is - how likely is it to occur, what resources do the attacker require and at what range can he succeed? The talks is intended to be a short overview of practical RFID security research. In other words, a discussion of selected attacks or security issues that have actually been implemented and demonstrated during the course of academic or industrial research.

Thursday 20th May 2010:
Speaker: Juan E. Tapiador (University of York, UK)
Title: Linear Cryptanalysis of Ultralightweight RFID Authentication Protocols
Abstract: In many RFID applications, authentication between tags and readers must be carried out without relying on traditional cryptographic primitives (e.g., PRF), as tags are assumed to be devices with very limited computational resources and therefore unable to implement them. One problem with many of the schemes recently proposed is that their security claims are backed only by informal arguments. While such arguments are generally useful, it is often the case that, though intuitive, they may be flawed. In this talk we introduce a novel cryptanalytic technique applicable to some of these protocols and prove its effectiveness against two recently proposed schemes: a protocol by Yeh, Lo, and Winata presented at RFIDSec'10 Asia, and a protocol by David and Prasard presented at MobiSec'09. In both cases, it is shown how a passive attacker can recover all the private information stored in the tag (i.e., secret keys and static identifier) after eavesdropping only a small number of authentication sessions.

Thursday 27th May 2010:
Speaker: Raphael Phan (Loughborough University, UK)
Title: Factoring Humans into Adversarial Notions
Abstract: We revisit the concept behind adversarial notions featured predominantly in security research, and discuss the relevance with real-world human-involved security contexts.

Thursday 3rd June 2010:
Speaker: Theo Tryfonas (University of Bristol, UK)
Title: Using Benford's Law to detect steganography
Abstract: The talk introduces a method of JPEG image steganalysis based on a generalised form of Benford's Law. Our approach is motivated by the need for quick detection of potential stego-carrier files with no prior knowledge of the steganography algorithm used, nor previous database of suspect carrier files available. The suspicious image is analysed in order to identify the encoding algorithm while various meta-data are retrieved. An image file is then reconstructed in order to be used as a comparison measure. A generalisation of the basic

principle of Benford Law's distribution is applied on both the source and the reconstructed file in order to detect whether the examined file is a stego-carrier file. We demonstrate the effectiveness of our technique by applying it on a new steganalytic tool that can blindly detect the use of JPHide/JPseek/JPHSWin, Camouflage and Invisible Secrets. Experimental results show that this method is able to detect the use of different steganography algorithms without the use of a time-consuming training step of neural networks, even if the embedding data rate is very low. The accuracy of our detector is independent of the payload. The method described can be extended in order to be used universally for the detection of different image format files which may act as stego-carriers.

Thursday 10th June 2010:
Speaker: Lars Knudsen (DTU, Denmark)
Title: Present Block Ciphers
Abstract: For most block cipher applications the AES is a good and preferred choice. However, AES it not well suited for extremely constrained environments such as RFID tags. One trend in block cipher design is to find ultra-lightweight block ciphers with good security and hardware efficiency. We present the ciphers Present (CHES 2007) and PrintCipher (CHES 2010). Another trend in block cipher design is to try to increase the efficiency by making certain components part of the secret key, e.g., to be able to reduce the number of rounds of a cipher. We cryptanalysed two such recent proposals, C2 (Crypto 2009) and Maya.

Thursday 17th June 2010:
Speaker: Julia Borghoff (DTU, Denmark)
Title: Bivium as a Mixed-0-1 Linear Programming Problem
Abstract: Trivium is a stream cipher proposed for the eSTREAM project. Raddum introduced some reduced versions of Trivium, named Bivium A and Bivium B. The problem of recovering an internal state of Bivium can be described as a system of quadratic Boolean equations. The problem of solving a system of quadratic equations over GF(2) is known to be NP-hard. We propose a new approach to solve such a system using combinatorial optimization. We convert the Boolean equation system into an equation system over R and formulate the problem of finding a 0-1-valued solution for the system as a mixed-0-1 programming problem. This gives us an attack on Bivium B in estimated time complexity of 2^64 seconds.

Friday 23rd July 2010 (note change of day for this week: the seminar will be on FRIDAY at 1PM, in room 229):
Speaker: Aggelos Kiayias (University of Athens, Greece)
Title: Encryption for Digital Content
Abstract: Encrypting digital content that is to be broadcasted to a set of receivers puts forth various interesting questions for cryptographic research including how one can utilize the available bandwidth optimally, how to trace key exposure incidents, and how to revoke exposed keys. The repeated failures of traditional cryptographic and security methods to solve these problems in practice, motivated a new class of cryptographic constructs that include broadcast encryption, traitor tracing, fingerprinting codes and others. In this lecture we will give a glimpse to this new cryptographic toolset and briefly discuss recent constructions and relevant security models.

Thursday 29th July 2010:
Speaker: Alexandra Boldyreva (Georgia Tech, USA)

Title: Deterministic encryption: theory and applications
Abstract: The focus of the talk is deterministic public-key encryption. Besides being interesting from theoretical and historical perspectives, the deterministic encryption primitive has applications to fast and secure search on remote data. We discuss several notions of security for deterministic encryption and relations among them. We present several constructions provably meeting these notions, based on various assumptions.

Thursday 02nd September 2010:
Speaker: Audun Jøsang (University of Oslo, Norway)
Title: Trust and Reputation Systems
Abstract: Trust and reputation systems are emerging as an important class of decision support tools for online activities and for assessing the risk of accessing online services. A general characteristic of reputation systems is that they provide global reputation scores, meaning that all the members in a community will see the same reputation score for a particular agent. On the other hand, trust systems can in general be used to derive local and subjective measures of trust, meaning that different agents can derive different trust in the same entity.

Trust and reputation systems pose several challenges in order to be practical and to provide reliable decision suport, such as robustness, semantics, privacy, and legality. This presentation gives an overview and discusses the challenges of trust and reputation systems.

The programme for the 2008/2009 academic year was as follows:

Monday 22nd September at 2pm:
Speaker: Dr. Christine O'Keefe (CSIRO, Australia)
Title: Analysing confidential data without compromising confidentiality
Abstract: As the healthcare industry moves from paper-based to electronic records, electronic data archives are accumulating in healthcare facilities and administrative agencies. Analysis of these health system usage and clinical data can yield information vital to effective health policy development and evaluation, as well as to enhanced clinical care through evidence-based practice and safety and quality monitoring.

At the same time, the analysis of these confidential health data archives must be conducted in such a way as not to compromise standards of privacy and confidentiality for individual health care consumers, health care providers, health care facilities and health data custodians. Privacy legislation and codes of practice must be adhered to as a minimum requirement and health data custodians' responsibilities to protect sensitive data must be supported.

In this talk I will provide a review of some technological approaches to the problem of enabling the use of health data for research and policy analysis while protecting privacy and confidentiality. Throughout the talk I will highlight the mathematical and statistical challenges and contributions, including the development of quantitative measures of disclosure risk and data utility.

Thursday 2nd October:
Speaker: Geong Sen Poh (ISG, RHUL)
Title: Watermarking Protocols for Tracing of Digital Content
Abstract: In this talk we give an overview on the construction of watermarking protocols and analyse a few examples of such protocols that aim at deterring dishonest clients from illegally

distributing copies of bought content. Differing from common watermarking schemes used for tracing of content, these protocols, in addition to giving the content distributor the capability to trace and identify these dishonest clients, also allow the content distributor to prove illegal acts to a third party. At the same time, an honest client is prevented from being falsely accused of illegal content distribution by the distributor. Many protocols have been proposed, and we shall examine two recent proposals. We will show that these proposals contain a number of flaws. We further put forward our thoughts on how it is possible to avoid the security weaknesses found in them.

Thursday 9th October:
Speaker: Maura Paterson (ISG, RHUL)
Title: Key Predistribution for Homogeneous Wireless Sensor Networks with Group Deployment of Nodes
Abstract: Recent literature contains proposals for key predistribution schemes for sensor networks in which nodes are deployed in separate groups. In this talk we consider the implications of group deployment for the connectivity and resilience of a key predistribution scheme. After showing that there is a lack of flexibility in the parameters of a scheme due to Liu, Ning and Du, limiting its applicability in networks with small numbers of groups, we propose a more general scheme, based on the structure of a resolvable transversal design. We demonstrate that this scheme permits effective trade-offs between resilience, connectivity and storage requirements within a group-deployed environment as compared with other schemes in the literature, and show that group deployment can be used to increase network connectivity, without increasing storage requirements or sacrificing resilience.

Thursday 16th October:
Speaker: Elizabeth Oswald (Bristol)
Title: Advances in Power Analysis Attacks
Abstract: Since the advent of power analysis attacks, researchers have set out to investigate different attack techniques, attack different algorithms and devices, and find (formal) ways to describe and analyse their findings. In this talk, I will review some of the results of the last 2-3 years made in these areas.

Thursday 23rd October:
Speaker: Praveen Gauravaram (DTU, Denmark)
Title: On-line birthday forgery attack on some RMX-hash-then-sign signature schemes
Abstract: At Crypto 2006, Halevi and Krawczyk proposed a message randomization algorithm called RMX as a front-end tool to the current hash-then-sign signature schemes such as DSS and RSA in order to free the reliance of these signature schemes on the collision resistance property of the hash functions. It has been proven that to break RMX-hash-then-sign signature scheme, one has to solve a cryptanalytical task which is related to finding second preimages for the compression function.

In this talk, an on-line birthday forgery attack on the RMX-hash-then-sign signature schemes that use the popular Davies-Meyer compression function (e.g., MD4, MD5, SHA family and Tiger) will be presented. This attack is also applicable to the signature schemes that use Davies-Meyer compression functions and a variant of RMX published by NIST in its latest Draft Special Publication (SP) 800-106.

Thursday 30th October:
Speaker: Geraint Price (ISG, RHUL)

Title: De-Perimeterisation: Fact or Fiction?
Abstract: It is undeniable that the security boundaries of organisations are changing. In response to this challenge, the Jericho Forum has set out a road-map for migration to a boundaryless security architecture. The culmination of the journey is seen as "security at the data level".

We cast a critical and dispassionate eye over the Forum's proposals. Our view is that their vision of the future is itself a panaceic utopia, unlikely to be achieved in reality. However, we do believe that much within their vision is built on sound principles. What's more, the Jericho Forum has brought much needed exposure to a real and evolving set of problems which need to be addressed by the Information Security community at large.

Thursday 6th November: No seminar

Thursday 13th November:
Speaker: Shane Balfe (ISG, RHUL)
Title: Trust Management for Secure Information Flows
Abstract: In both the commercial and defence sectors a compelling need is emerging for the rapid, yet secure, dissemination of information across traditional organisational boundaries. In this talk we present a novel trust management paradigm for securing pan-organisational information flows that aims to address the threat of information disclosure. Our trust management system is built around an economic model and a trust-based encryption primitive wherein: (i) entities purchase a key from a Trust Authority (TA) which is bound to a voluntarily reported trust score r, (ii) information flows are encrypted such that a flow tagged with a recipient trust score R can be decrypted by the recipient only if it possesses the key corresponding to a voluntarily reported score r <= R, (iii) the economic model (the price of keys) is set such that a dishonest entity wishing to maximise information leakage is incentivised to report an honest trust score r to the TA. This paper makes two important contributions. First, we quantify fundamental tradeoffs on information flow rate, information leakage rate and error in estimating recipient trust score R. Second, we present a suite of encryption schemes that realise our trust-based encryption primitive and identify computation and communication tradeoffs between them.

Thursday 20th November:
Speaker: Nigel Boston (UCD, Dublin)
Title: Stylometric Watermarking
Abstract: Stylometry is mathematical analysis of a literary piece in order to determine authorship. A stylometric watermarking is a `style' added to a piece to prove ownership. This is joint work with Qian Zhang (Microsoft Research).

Thursday 27th November:
Speaker: Eike Kiltz (CWI, Amsterdam)
Title: Practical Chosen Ciphertext Secure Encryption from Factoring
Abstract: We propose a new public-key encryption scheme whose (standard model) security against adaptive chosen-ciphertext attack is equivalent to the factoring assumption. The scheme is quite practical as its encryption/decryption algorithms only perform two modular exponentiations. To the best of our knowledge, this is the first scheme that simultaneously enjoys these two properties. Joint work with D. Hofheinz (CWI).

Thursday 4th December:
Speaker: Jon Callas (PGP Corporation)
Title: Virtual economies and e-cash
Abstract: What's virtual about a virtual economy, especially if it involves real money? What makes e-cash cash? We'll discuss these questions, what they can tell us about the "real" economies, as well as how they are constructed, and how they are viable or not as economies and cash.

Thursday 11th December:
Speaker: Ana Ferriera (University of Kent at Canterbury)
Title: Access Control in Healthcare Information Systems

Thursday 15th January:
Speaker: Jason Crampton (ISG, RHUL)
Title: Mathematical Representation and Interpretation of Authorization Policies
Abstract: Existing ``target-based" approaches for constructing authorization policies suffer from significant shortcomings, mainly because they do not make a proper distinction between authorization state and authorization policy. We propose an alternative approach in which an authorization policy is a function and authorization state is one or more inputs to a policy. We use two policy operators to construct more complex policies from existing policies. We show how our approach can be used to encode XACML policies and discuss the advantages of our approach over existing approaches.

Thursday 22nd January: Cancelled!

Thursday 29th January: No seminar

Thursday 5th February:
Speaker: Mark Ryan (University of Birmingham)
Title: Attacks on the Trusted Platform Module, and solutions
Abstract: The Trusted Platform Module (TPM) is a hardware chip designed to enable computers achieve greater security. Proof of possession of values known as authData is required by user processes in order to use TPM keys. We demonstrate two attacks relating to the way authData is handled, and explain their consequences. By using the attacks, an attacker can circumvent some crucial operations of the TPM, and impersonate a TPM user to the TPM, or impersonate the TPM to its user. We describe modifications to the TPM protocols that avoid these attacks, and use protocol verification techniques to prove their security. I also hope to give some ideas for future research in trusted computing. Joint work with Liqun Chen (HP Labs).

Thursday 12th February:
Speaker: Andrew D. Gordon (Microsoft Research, Cambridge)
Title: Principles and Applications of Refinement Types
Abstract: A refinement type is a type qualified by a logical constraint; an example is the type of even numbers, that is, the type of integers qualified by the is-an-even-number constraint. Although this idea has been known in the research community for some time, it has been assumed impractical, because of the difficulties of constraint solving. But recent advances in automated reasoning have overturned this conventional wisdom, and transformed the idea into a practical design principle. I will present a primer on the design, implementation, and application of refinement types. I will explain:

How a range of diverse features may be unified as instances of the general idea of refinement types.

How a static checker for the Oslo modeling language M allows us to check for security errors in server configurations; intended constraints on configurations are expressed with refinement types, so that configuration validation reduces to type checking.

How we statically check integrity and secrecy properties of security critical code, such as an implementation of the CardSpace security protocol, using a system of refinement types for the F# programming language.

My lecture is based on recent research with my esteemed colleagues Karthik Bhargavan, Gavin Bierman, and Cédric Fournet of MSR Cambridge, and David Langworthy of the Microsoft Connected Systems Division; much of our work relies on the excellent Z3 automated theorem prover developed by Nikolaj Bjorner and Leonardo de Moura of MSR Redmond.

Thursday 19th February:
Speaker: Dario Catalano (Università di Catania)
Title: Verifiable Random Functions from Identity-based Key Encapsulation
Abstract: We propose a methodology to construct verifiable random functions from a class of identity based key encapsulation mechanisms (IB-KEM) that we call VRF suitable. Informally, an IB-KEM is VRF suitable if it provides what we call unique decryption (i.e. given a ciphertext C produced with respect to an identity ID, all the secret keys corresponding to identity ID', decrypt to the same value, even if ID\neq ID') and it satisfies an additional property that we call pseudorandom decapsulation. In a nutshell, pseudorandom decapsulation means that if one decrypts a ciphertext C, produced with respect to an identity ID, using the decryption key corresponding to any other identity ID' the resulting value looks random to a polynomially bounded observer. Interestingly, we show that most known IB-KEMs already achieve pseudorandom decapsulation. Our construction is of interest both from a theoretical and a practical perspective. Indeed, apart from establishing a connection between two seemingly unrelated primitives, our methodology is direct in the sense that, in contrast to most previous constructions, it avoids the inefficient Goldreich-Levin hardcore bit transformation.

Joint work with Michel Abdalla and Dario Fiore.

Thursday 26th February:
Speaker: Steve Schneider (University of Surrey)
Title: Secure Electronic Voting
Abstract: Elections need to be trustworthy, and to be seen to be trustworthy, in order for the electorate to have confidence in their outcomes. The introduction of technology into the electoral process brings potential new benefits, but may also increase the risk that accidental flaws or security weaknesses in the equipment leave an election open to tampering. Voting systems, whether run manually or on machines, should provide voters with the ability to cast a private vote, and to have confidence that their vote is really included in the final tally.

The Prêt à Voter electronic voting system is designed to provide these properties, and some further ones known as end-to-end verifiability, not currently present in standard UK elections: a receipt for the voters so that they can check their vote has been included in the tally, and can prove if it has not; and publication of the votes so that the count can be independently checked. This is achieved by making public all the stages in the processing of the votes, enabling the election to be audited independently. All this is possible while maintaining secrecy of the vote. Although electronic support for the election is necessary, the electronic components do not themselves need to be trusted because their outputs can be independently audited. This talk discusses the issues involved in electronic voting systems, describes the Prêt à Voter approach to electronic voting, and introduces the implementation of the system developed at the University of Surrey in conjunction with the University of Newcastle in 2007.

Thursday 5th March:
Speaker: Alex Dent (RHUL)
Title: Constructing signcryption schemes
Abstract: A signcryption scheme is a public-key scheme which "encrypts" messages in a way that combines the advantages of public-key encryption scheme and a digital signature scheme. It is supposed to provide confidentiality, integrity protection, and origin authentication. The idea is to do this in a way that has some significant advantage over a combination of encryption and signing. This advantage could be in security, computational complexity, or bandwidth efficiency. The best schemes combine all three advantages.

There are essentially three ways of constructing a signcryption schemes: using encryption-then-sign techniques; using ECIES techniques and the random oracle model; and applying the CHK transform to an identity-based signcryption scheme. In all of these construction paradigms, one typically starts with a signature scheme and converts this to a signcryption scheme. In this talk, we will look at the advantages and disadvantages of the existing construction paradigms, and present two new construction paradigms which take their inspiration from encryption schemes rather than signature schemes.

Thursday 12th March at 3pm (please note time):
Speaker: Gaven Watson (RHUL)
Title: Plaintext recovery attacks against SSH
Abstract: Alongside SSL/TLS and IPsec, SSH is one of the most widely used secure protocol suites. It was originally designed as a replacement for insecure remote login procedures such as rlogin and telnet. It has since become a general purpose tool for securing Internet traffic. In this talk, I will describe plaintext recovery attacks against SSH. The attacks have been implemented against OpenSSH, where we can verifiably recover 14 bits of plaintext from an arbitrary block of ciphertext with probability 2^{-14} and 32 bits of plaintext from an arbitrary block of ciphertext with probability 2^{-18}. I will explain why a combination of flaws in the basic design of SSH leads implementations such as OpenSSH to be vulnerable to the attacks, why the current provable security analysis for SSH fails to capture the attacks, and how the attacks can be prevented in practice. Joint work with Martin Albrecht and Kenny Paterson.

Thursday 19th March:
Speaker: Jens Groth (UCL)
Title: Pairing-based non-interactive zero-knowledge proofs
Abstract: Non-interactive zero-knowledge proofs make it possible to prove the truth of a statement without revealing any other information. They have been used widely in the theory of cryptography, but due to efficiency problems have not yet found many practical applications. In this talk, we will cover recent pairing-based constructions of non-interactive

zero-knowledge proofs that yield the necessary efficiency for practical applications as well as the possibility to have perfect and everlasting privacy.

Friday 20th March at 4.30pm - extra seminar:
Speaker: Paul Karger (IBM)
Titles: High Assurance Smart Cards for Multinational Coalitions and Other Applications of National Security AND Securing Virtual Machine Monitors: What is Needed?
Abstract: Caernarvon is a high-assurance secure operating system for smart cards, designed to pass the highest levels (EAL7) of the Common Criteria. It includes a multi-organizational mandatory access control model that is designed to provided both security and integrity controls that can scale to cover the entire Internet. These multi-organizational controls can make it much easier to implement applications for multi-national military, electronic visas that could be stored on the same smart card chip as is used for electronic passports.

Wednesday 25th March at 3pm - extra seminar:
Speaker: Paulo Barreto (University of São Paulo)
Title: Syndrome-based Post-quantum Crypto

Thursday 26th March:
Speaker: Sebastian Gajek (Bochum)
Title: Universally Composable Delegated Authentication Secure Communication Sessions Resilient against Credential Compromise
Abstract: We consider the problem of building delegated authentication secure sessions (DAS) protocols, where the client first runs a secure communication sessions (SCS) protocol with a trusted server using a password in order to retrieve authentication credentials for the establishment of another mutually authenticated secure session with the destined server. DAS protocols have gained much attention. They are a key ingredient in (federated) identity management systems (e.g. Google's SSO, Microsoft's CardSpace) which turned out to be vulnerable: It is desirable to maintain some level of security even if the attacker has compromised the credential. A DAS protocol is said to be resilient against credential compromise if an adversary (although he knows the credential) must at least perform an online password dictionary attack in order to impersonate the client.

We adapt the secure channel model from Canetti and Krawczyk [Eurocrypt, 2002] to the setting where the client identity may remain undisclosed and in addition a higher-layer protocol mediates credentials between the session instances. We prove security in the universal composability framework by (1) defining a new functionality for DAS with resilience to credential compromise, (2) defining a new binding secure sessions functionality, (3) specifying a protocol combining this binding with a basic SCS functionality, (4) proving that this protocol securely realizes the new functionality for DAS, and (5) demonstrate the applicability in the browser-server setting.

Thursday 23rd April:
Speaker: Alf Zugenmaier (DOCOMO Eurolabs, Germany)
Title: Security in Network Virtualization
Abstract: Network virtualization is a relatively new research topic. A number of papers propose that certain benefits can be realized by virtualizing links between network elements as well as adding virtualization on intermediate network elements. This talk will first give an introduction to the design space of network virtualization and then discuss some potential security issues with and potential security benefits of using network virtualization.

Thursday 30th April in McCrea Room 219:
Speaker: Carlo Gebhardt (ISG, RHUL)
Title: Trusted Execution Technology
Abstract: Trusted Execution Technology (TXT), formally named LaGrande, is a set of hardware extensions, introduced by Intel, to defend against software attacks against an Intel based platform. TXT is a good example of how Trusted Computing and virtualisation are merging: Hardware virtualisation support in the CPU and chipset is extended by a Trusted Platform Module (TPM), to provide trusted and sealed storage as well as reporting platform attestation. Consequently, this talk seeks to explain the concepts of TXT as well as highlighting its importance for virtualisation as well as Trusted Computing. Moreover, this talk will also present the concepts of the TXT prototype developed in corporation with HP labs Bristol.

Thursday 7th May:
Speaker: Renato Renner (ETH, Zurich)
Title: Quantum attacks against non-quantum cryptosystems
Abstract: It is well known that standard cryptographic systems whose security is based on the (assumed) hardness of factoring can be broken with the help of a quantum computer. Somewhat surprisingly, a similar problem may also arise for cryptosystems that do not rely on computational assumptions. In this talk, I will show that there exist cryptographic schemes which provide information-theoretic security in a "classical" (in the sense of "non-quantum") world, but nevertheless are insecure against attackers that use quantum mechanics. This implies that security proofs based on standard (non-quantum) information theory cannot generally be considered complete.

Thursday 14th May:
Speaker: Gary McGuire (UCD, Ireland)
Title: On the construction using complex multiplication of genus 1 and genus 2 curves for cryptography
Abstract: We will survey the complex multiplication method for constructing elliptic and genus 2 curves suitable for cryptography. In particular we will discuss genus 2 curves that are neither ordinary nor supersingular. We may also mention the construction of pairing-friendly curves of this type.

Thursday 21st May:
Speaker: Sondre Ronjom (University of Bergen, visiting RHUL)
Title: Nonlinear equivalence of stream ciphers over GF(q)
Abstract: Boolean functions play very important roles in cryptography and are essential providers of non-linearity in many cryptographic primitives. A significant amount of literature has been devoted to the analysis of cryptographic properties of Boolean functions. Cryptanalysis utilizing weak such properties include correlation attacks, algebraic attacks, inversion attacks, among others. A filter generator is a stream cipher in its simplest form and has a well-defined mathematical description. It is a fundamental construction, and consists of a sequence generator and a nonlinear Boolean function. Several stream ciphers in literature can be seen as extensions of such a generator. Thus, investigating the cryptographic properties of the filter generator is important for understanding the properties of even more complex systems.

The purpose of this talk is to investigate nonlinear equivalences of LFSR-based stream ciphers using basic properties of Galois fields and a nonlinear change of basis. The focal point is then that many important cryptographic properties of Boolean functions which remains variant with respect to affine transformations, does not with respect to a nonlinear change of basis. Thus, while one stream cipher may have very good cryptographic properties, there may very-well exist a non-linearly equivalent stream cipher which may be weak with respect to some cryptographic property. It then becomes evident that there is a need for generalizing cryptographic properties (and constructions) in order to take such nonlinear equivalences into account.

Thursday 28th May:
Speaker: Stephen Wolthusen (ISG, RHUL)
Title: State Estimation and Prediction for Intrusion Detection in Distributed Control Systems
Abstract: Supervisory Control and Data Acquisition (SCADA) systems are increasingly required for the operation of many types of critical infrastructure. Site-specific properties of SCADA environments make subversion detection impractical while conventional anomaly detection will be degraded owing to sensor noise and feedback characteristics. We propose a sequential Monte Carlo model using importance sampling based on an explicit control law model to capture the nonlinear and non-Gaussian behavior of the underlying system and to identify multivariate anomalies among sensor and actuator data.

Thursday 4th June:
Speaker: Jeff Yan (Newcastle)
Title: The robustness of CAPTCHAs

Abstract: No matter whether you like or hate it, CAPTCHA has found widespread application on numerous commercial web sites - it is now almost a standard security mechanism for defending against undesirable or malicious Internet bot programs.

This talk introduces our recent work on attacking numerous widely deployed CAPTCH As. I will present new techniques of general value to attack a number of text CAPTCH As, including the schemes designed and deployed by Microsoft, Yahoo and Google. In particular, the Microsoft CAPTCHA has been deployed since 2002 at many of their online services including Hotmail, MSN and Windows Live. Designed to be segmentation-resistant, this scheme has been studied and tuned by its designers over the years. However, our simple attack has achieved a segmentation success rate of higher than 90% against this scheme. It took on average ~80 ms for the attack to completely segment a challenge on an ordinary desktop computer. As a result, we estimate that this CAPTCHA could be instantly broken by a malicious bot with an overall (segmentation and then recognition) success rate of more than 60%. On the contrary, the design goal was that automated attacks should not achieve a success rate of higher than 0.01%. For the first time, our work shows that CAPTCH As that are carefully designed to be segmentation-resistant are vulnerable to novel but simple attacks.

Our experience suggests that CAPTCHA will go through the same process of evolutionary development as cryptography, digital watermarking and the like, with an iterative process in which successful attacks lead to the development of more robust systems.

Thursday 11th June at 3pm:
Speaker: Craig Gentry (Stanford and IBM)
Title: Fully Homomorphic Encryption Using Ideal Lattices
Abstract: We propose a fully homomorphic encryption scheme -- i.e., a scheme that allows one to evaluate circuits over encrypted data without access to the decryption function. First,

we provide a general preliminary result -- that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call such a scheme bootstrappable. Next, we provide a bootstrappable public key encryption scheme using ideal lattices.

Thursday July 2nd:
Speaker: Rei Safavi-Naini (Calgary)
Title: Random key pre-distribution for sensor networks with security against node capture
Abstract: Random key pre-distribution schemes provide an elegant solution to the problem of secure key establishment in resource constrained sensor networks. We revisit security of these schemes against an adversary who can capture a number of nodes in the network, and show that guaranteed security can only be obtained at very high communication cost. We then propose a new approach that provides security against such adversaries with only a small additional communication cost. We show the security guarantee of this system analytically and also through extensive simulations.

Thursday July 9th:
Speaker: Doug Stinson (Waterloo)
Title: Practical Unconditionally Secure Two-channel Message Authentication
Abstract: We investigate unconditional security for message authentication protocols that are designed using two-channel cryptography. We look at both noninteractive message authentication protocols (NIMAPs) and interactive message authentication protocols (IMAPs). We provide a new, short proof of nonexistence of nontrivial unconditionally secure NIMAPs. This proof consists of a combinatorial counting argument. Further, we propose a generalization of an unconditionally secure 3-round IMAP due to Naor, Segev and Smith. With a careful choice of parameters, our scheme improves that of Naor et al. Our scheme is very close to optimal for most parameter situations of practical interest.

Friday 14th August at 10.30am:
Speaker: Peter Martini (Bonn)
Title: Cyber Defense - Unprotected in a Networked World?
Abstract: In recent years, cybercrime has become big business - really big business. Computers are infiltrated by spyware, computers are hijacked to serve some distant master's will, and computers are subject to denial of service attacks. The cyber defense team at the University of Bonn, Germany, claims that reactive countermeasures are important - but not enough. This claim is substantiated by recent experiences gained by deep malware analysis, i.e. by dissecting malware such as "Storm", "Kraken" and "Conficker". The presentation discusses the situation observed at honeypots, highlights characteristics of modern botnets, and addresses both "classical" (= reactive) and "proactive" countermeasures.

Speaker: Boaz Tsaban (Bar-Ilan University, Israel)
Title: Length-based algorithms in noncommutative groups
Abstract: At present, there are few public-key schemes which are considered secure. All of them are based on commutative groups. Most of them can be broken in subexponential time using standard computers, and all of them can be broken in polynomial time using quantum computers. About 10 years ago, an investigation began of the potential of basing a public-key scheme on a noncommutative algebraic structure. Thus far, most of the proposed systems of this kind supply the eavesdropper with equations in the underlying group, whose solutions leads to breaking the scheme. The equations are usually generated in a very specific way:

independent, identically distributed elements of the group are chosen, and their multiplication (disguised by using a normal form in the group) is sent in the air. We describe a simple generic approach ("memory-length" algorithms), to solve such equations in a heuristic manner. This approach was developed several years ago with a team of researchers from BIU (Garber, Kaplan, Teicher, Vishne) and recently improved with Ruinskiy and Shamir (WIS). We demonstrate the successfulness of this approach by experiments conducted on a cryptosystem of Shpilrain and Ushakov, which uses Thompson's group F as its platform. We then describe a new variant of this approach, which shows great promise for further investigations. The talk is mainly heuristic, no advanced mathematical knowledge is required. Students are especially welcome. Joint work with Dima Ruinskiy and Adi Shamir.

Wednesday 2nd September in McCrea 219 at 4pm:
Speaker: Boaz Tsaban (Bar-Ilan University, Israel)
Title: Cryptanalysis of the Algebraic Eraser Cryptography Scheme
Abstract: In March 2004, Anshel, Anshel, Goldfeld, and Lemieux introduced the 'Algebraic Eraser' scheme for key agreement over an insecure channel, using a novel hybrid of infinite and finite noncommutative groups. They also introduced the 'Colored Burau Key Agreement Protocol' (CBKAP), a concrete and very efficient realization of this scheme. We present general, efficient heuristic algorithms, which extract the shared key out of the public information provided by CBKAP. These algorithms are, according to heuristic reasoning and according to massive experiments, successful for all sizes of the security parameters, assuming that the keys are chosen with standard distributions. Our methods come from probabilistic group theory, and have not been used before in cryptanalysis. In particular, we provide a simple and very efficient heuristic algorithm for finding short expressions of permutations in S_n, as products of given random permutations. Our algorithm gives expressions of length O(n^2log n), in time O(n^4log n) and space O(n^2log n), and is the first practical one for n > 128. The talk is self-contained, no advanced mathematical knowledge is required. Students are especially welcome.

Thursday 3rd September in McCrea 229 at 4pm:
Speaker: Elisavet Konstantinou (University of the Aegean)
Title: Pairings in cryptography: from the selection of their parameters to their application in group key agreement protocols
Abstract: Recent years have seen an explosion of interest in pairing based cryptography. Ranging from number theorists to security practitioners, this particular field of public key cryptography is for all challenging and fascinating. In this talk, we will try to present aspects of pairing based cryptography from both these extreme points of view. Connecting cryptography with algebraic number theory, we will show how Ramanujan's work can influence the selection of pairing-friendly curves. On the other hand, treating pairings as "black boxes" and moving to network security area, we will present a pairing-based group key agreement protocol, particularly suitable for mobile ad-hoc networks.

The programme for the second semester of the 2007/2008 academic year was as follows:

Thursday 10th January:
Speaker: Colin Boyd (QUT, Australia)
Title: Towards Non-Parallelizable Client Puzzles
Abstract: Client puzzles have been proposed as a useful mechanism for mitigating denial of service attacks on network protocols. Several different puzzles have been proposed in recent years. The first half of this talk will review the desirable properties of client puzzles and

existing puzzle proposals. The second half will investigate how to provide the property of non-parallelizability in a client puzzle. A new puzzle based on the subset sum problem will be described. Despite some practical implementation issues, this is the first example that satisfies all known desirable properties for a client puzzle. This is joint work with Suratose Tritilanunt, Ernest Foo and Juan Gonzalez.

Thursday 17th January:
Speaker: Richard Gopaul (Army Research Laboratory, USA)
Title: Countering False Accusations and Collusion in the Detection of In-Band Wormholes
Abstract: Cooperative intrusion detection techniques for MANETs rely on using ordinary computing hosts as network intrusion sensors. If compromised, these hosts may inject artificial data into the intrusion detection system to hide their presence while attacking or falsely accuse well-behaved nodes. Byzantine fault tolerance approaches involving voting are potentially applicable, but must address the fact that only nodes in particular topological locations at particular times are qualified to vote on whether an attack occurred. We examine these issues in the context of a prototype distributed detector for self-contained, inband wormholes in OLSR networks. We propose an opportunistic voting algorithm and present test results from a 48-node testbed in which colluding attackers generate corroborating false accusations against pairs of innocent nodes. The results indicate that opportunistic voting can instantaneously suppress false accusations when the network topology and routes chosen by OLSR provide a sufficient number of nearby honest observers to outvote the attackers. Techniques employed for data aggregation and optimization will also be discussed.

Thursday 24th January:
Speaker: Bogdan Warinschi (University of Bristol)
Title: Computational Soundness - An Introduction
Abstract:
Computationally sound symbolic analysis of security protocols has recently emerged as a promising new approach in dealing with the complexities of typical cryptographic proofs. The approach tries to bridge the gap between the symbolic (Dolev-Yao style) methods and tools, and the computational methods of modern cryptography with the goal of obtaining the best of both worlds: machine-checkable, (semi)-automated security proofs that offer strong computational guarantees.

This talk is a gentle, example-based, introduction to the tools and methods of computational soundness. I will focus on the simpler case of passive adversaries (i.e. adversaries that can not interfere with the communication between parties), but I will also provide a short overview of other existing research directions that fall under the name of computational soundness.

Thursday 31st January:
Speaker: Carles Padro (Technical University of Catalonia)
Title: Ideal Multipartite Secret Sharing Schemes
Abstract: Multipartite secret sharing schemes are those having a multipartite access structure, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role. Several particular families of multipartite schemes, such as the weighted threshold schemes, the hierarchical and the compartmented schemes, and the ones with bipartite or tripartite access structure have been considered in the literature. The characterization of the access structures of ideal secret sharing schemes is one of the main open problems in secret sharing. In this work, the characterization of ideal multipartite

access structures is studied with all generality. Our results are based on the well-known connections between ideal secret sharing schemes and matroids.

One of the main contributions of this paper is the application of discrete polymatroids to secret sharing. They are proved to be a powerful tool to study the properties of multipartite matroids. In this way, we obtain some necessary conditions and some sufficient conditions for a multipartite access structure to be ideal. Our results can be summarized as follows. First, we present a characterization of matroid-related multipartite access structures in terms of discrete polymatroids. As a consequence of this characterization, a necessary condition for a multipartite access structure to be ideal is obtained.

Second, we use linear representations of discrete polymatroids to characterize the linearly representable multipartite matroids. In this way we obtain a sufficient condition for a multipartite access structure to be ideal. Finally, we apply our general results to obtain a complete characterization of ideal tripartite access structures, which was until now an open problem.

Thursday 7th February :
Speaker: Keith Martin (ISG, RHUL)
Title: Challenging the adversary model in secret sharing schemes
Abstract: Secret sharing schemes are cryptographic primitives for distributing shares of a secret amongst a set of entities in such a way that only certain coalitions can reconstruct the secret from their shares. Secret sharing schemes are highly versatile primitives that are particularly useful in applications where there is no single point of trust. The traditional secret sharing model makes the important assumptions that there is a trusted dealer, adversaries are passive and participants behave in a polarised manner (they are either honest or malicious). These assumptions are reasonable in some situations, but do not necessarily map comfortably onto many application environments. We will present a ``birds-eye" view of research on secret sharing schemes, concentrating on research that has challenged this traditional adversary model.

Thursday 14th February:
Speaker: Chris Mitchell (ISG, RHUL)
Title: Cryptanalysis of the EPBC Authenticated Encryption Mode
Abstract: A large variety of methods for using block ciphers, so called 'modes of operation', have been proposed, including some designed to provide both confidentiality and integrity protection. Such modes, usually known as 'authenticated encryption' modes, are increasingly important given the variety of issues now known with the use of unauthenticated encryption. In this paper we show that a mode known as EPBC (Efficient error-Propagating Block Chaining), proposed in 1997 by Zúquete and Guedes, is insecure. Specifically we show that given a modest amount of known plaintext for a single enciphered message, new enciphered messages can be constructed which will pass tests for authenticity. That is, we demonstrate a message forgery attack.

Thursday 21st February:
Speaker: Martin Albrecht (RHUL)
Title: Algebraic Techniques in Differential Cryptanalysis
Abstract: We propose a new cryptanalytic method against block ciphers, which combines both algebraic and statistical techniques. More specifically, we show how to use algebraic relations arising from differential characteristics to speed up and improve key-recovery

differential attacks against block ciphers in some situations. To illustrate the new technique, we apply it to reduced round versions of the cipher PRESENT, an ultra lightweight block cipher proposed at CHES 2007, particularly suitable for deployment in RFID tags.

Friday 22nd February:
Speaker: Jesse Walker (Intel)
Title: 802.16e security
Abstract: This talk gives an overview of the security mechanisms described by the 802.16e standard.

Thursday 28th February:
Speaker: Peter Ryan (University of Newcastle)
Title: Advances in Verifiable Voting Schemes
Abstract: Significant progress has been made in recent years in the developement and evaluation of verifiable voting schemes. In this talk I outline the Pret a Voter approach to achieving voter-verifiability and various threats and vulnerabilities that have been identified in early versions of the scheme. I will describe recent enhancements that have been developed in response to these threats.

Thursday 6th March:
Speaker: Guilin Wang (University of Birmingham)
Title: Nominative Signatures
Abstract: Nominative signature is a new type of digital signatures. In such a scheme, a nominator (i.e. the signer) and a nominee (i.e. a designated verifier) jointly generate and publish a signature so that only the nominee can check the validity of a nominative signature and further convince a third party to accept this fact later. In this talk, we will first discuss the defintions and applications of nominative signatures. Then, we will analyze the security of an exisitng scheme by demonstrating some attacks. Finally, we will review two secure constructions of nominative signatures.

Thursday 13th March:
Speaker: Steven Galbraith (RHUL)
Title: An analysis of the vector decomposition problem
Abstract: The vector decomposition problem (VDP) has been proposed as a computational problem on which to base the security of public key cryptosystems. We give a generalisation and simplification of the results of Yoshida on the VDP. We then show that, for the supersingular elliptic curves which can be used in practice, the VDP is equivalent to the computational Diffie-Hellman problem (CDH) in a cyclic group. For the broader class of pairing-friendly elliptic curves we relate VDP to various co-CDH problems and also to a generalised discrete logarithm problem 2-DL which in turn is often related to discrete logarithm problems in cyclic groups. (Joint work with Eric Verheul.)

Thursday 20th March:
Speaker: Helger Lipmaa (UCL Ad Astral)
Title: On Some Open Problems in Communication-Efficient Cryptocomputing
Abstract: We will give an overview of a recent cryptocomputing method that makes it possible to cryptocompute every language in NC1. We give several nontrivial applications, including: (a) An (n,1)-CPIR protocol with log-squared communication and sublinear server-computation by giving a secure function evaluation protocol for Boolean functions with similar performance, (b) A protocol that makes it possible to compute (say) how similar is

client's input to an element in server's database, without revealing any information to the server, (c) A protocol for private database updating with low amortized complexity.
Paper: Cryptology ePrint Archive Report 2008/107.

Thursday 27th March:
Speaker: Geraint Price (ISG, RHUL)
Title: The Emperor's New Clothes: the danger of relying on "strong" authentication
Abstract: In this talk we will outline some of the difficulties faced by those implementing security protocols in distributed systems. Many designers of cryptographic primitives assume the pre-existence of a cryptographic means of bootstrapping the authentication phase of a protocol. In real world distributed systems this is not always feasible. To many in the security research community weaker notions of authentication are to be dismissed without further thought when proposing security designs. We will argue that building supposedly "secure" protocols on a false assumption of a non-existent strong authentication mechanism is just as dangerous, if not more so, as using a weak authentication primitive. In presenting our case, we hope to stimulate a debate which centres on the notion that, for some applications and security mechanisms, security researchers need to embrace other forms of achieving their goals than is currently the accepted gospel.

Thursday 3rd April: No seminar

Thursday 10th April:
Speaker: Alex Dent (ISG, RHUL)
Title: A Brief History of Provable-Secure Public-Key Encryption
Abstract: Public-key encryption schemes are a useful and interesting field of cryptographic study. The ultimate goal for the cryptographer in the field of public-key encryption would be the production of a very efficient encryption scheme with a proof of security in a strong security model using a weak and reasonable computational assumption. This ultimate goal has yet to be reached.

In this talk, we will survey some of the major attempts to solve this problem in a way that will (hopefully) be accessible to a general audience.

Thursday 17th April: No seminar

Thursday 24th April:
Speaker: Greg Neven (K.U. Leuven)
Title: Efficient sequential aggregate signed data
Abstract: This talk will give an overview of different approaches to bandwidth-saving signature primitives, and go into detail on a recent result presented at Eurocrypt 2008. Namely, we generalize the concept of sequential aggregate signatures (SAS) to a new primitive called sequential aggregate signed data (SASD) that tries to minimize the total amount of transmitted data, rather than just signature length. We present SAS and SASD schemes that offer numerous advantages over existing schemes, including having instantiations based on low-exponent RSA and factoring, drastically reducing signing and verification costs, and supporting aggregation of signatures under keys of different lengths. We also present a multi-signed data scheme that, when compared to the state-of-the-art multi-signature schemes, is the first with non-interactive signature generation that is not based on pairings.

Thursday 1st May:
Speaker: Ali Miri (School of Information Technology and Engineering and Department of Mathematics and Statistics, University of Ottawa)
Title: Accelerating Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields
Abstract: In this talk, we discuss various methodologies that we have developed to accelerate scalar multiplication on ECC over prime fields. We present a new methodology to derive faster composite operations of the form dP + Q, and in particular, an efficient Doubling-Addition (DA) operation. We present a flexible technique that uses the substitution of multiplication with squaring and other cheaper operations, exploiting the fact that field squaring is generally less costly than multiplication. We show the significant impact of this approach in sequential and parallel implementations that also includes protection against Simple Side-Channel Attacks (SSCA). We also present a new method for scalar multiplication that uses a generic multibase representation to reduce the number of required operations.
We show, that using an efficient NAF-like algorithm, conversion to such representations is sublinear in terms of the number of nonzero terms, and that it can be done without impacting memory or speed. (Joint work with Patrick Longa.)

Thursday 8th May:
Speaker: Seminar postponed
Title:

Thursday 15th May:
Speaker: Nathan Lea (Centre for Health Informatics and Multiprofessional Education, University College London)
Title: Experience of Managing Information Security in a Clinical
eScience Project
Abstract: The Clinical eScience Framework (CLEF) Project is a research project funded by the Medical Research Council and has been running since 2003. The CLEF Consortium consists of five research groups across four United Kingdom Colleges. The Consortium members have been researching computational methods for the storage, querying, protection and analysis of clinical information using a set of electronic data from approximately 22,500 deceased cancer patients' records treated at the Royal Marsden Hospital. As part of an ethics committee approvals process, the names, hospital numbers and addresses of the patients were removed from the records before they were released to the Project. The Consortium appreciated the sensitivity of the data and discovered that its potential for identifying patients was still a significant factor, and whilst there was a clear stipulation that patients should not be identified, there was limited guidance on how to manage that requirement. As a result, the challenge of protecting the information in a project that had users distributed nationally and all using different computational techniques as part of the eScience Initiative became a major research area for the Consortium. The Seminar today will look at the experience of managing information security in this project, the methods used, the issues that arose and how they were handled.

Thursday 22nd May:
Speaker: John Clark (University of York)
Title: Uses of Heuristic Search in Cryptography and its Applications
Abstract: In this talk I will indicate how heuristic non-linear search approaches have been used to provide competitive results in both crypto-component design and also analysis. Heuristic search is shown to be capable to generating Boolean functions with excellent

property profiles, of generating protocols designs to meet specifications. On the analysis side direct targets include the developmentof powerful approxinmatons. One of the most interesting developments has been the profiling of solving routines, where the search trajectory reveals more information than the final "result" of an attempted search. There is scope for the use of such approaches more generally in discrete mathematics (e.g. on Venn diagram problems or knot equivalence).

Thursday 29th May:
Speaker: Carlo Gebhardt (ISG, RHUL)
Title: Introduction to the security challenges of virtualization.
Abstract: Virtualization is not a new technology, but has recently experienced a resurgence of interest among industry and research. New products and technologies are emerging quickly, and are being deployed with little considerations to security concerns. It is vital to understand that virtualization does not improve security by default. Virtualization is a changeable and very dynamic field with an uncertain outcome. Hence, any aspect of virtualization needs to undergo constant security analysis and audit. This talk will discuss the unique security challenges of virtualization and illustrate the significance of ongoing security analysis in this area.

Thursday 5th June:
Speaker: Carsten Rudolph (Fraunhofer – Institute for Secure Information Technology SIT, Darmstadt)
Title: Security evaluation of scenarios based on the TCG's TPM Specification
Abstract: The Trusted Platform Module TPM is a basic but nevertheless very complex security component that can provide the foundations and the root of security for a variety of applications. In contrast to the TPM, other basic security mechanisms like cryptographic algorithms or security protocols have frequently been subject to thorough security analysis and formal verification. This talk presents a methodic security analysis of a large part of the TPM specification. A formal automata model based on asynchronous product automata APA and a finite state verification tool SHVT are used to emulate a TPM within an executable model. On this basis four different generic scenarios were analysed with respect to security and practicability: secure boot, secure storage, remote attestation and data migration. A variety of security problems and inconsistencies was found. Subsequently, the TPM specification was adapted to overcome the problems identified. In this talk, the general approach used by Fraunhofer SIT to validate specifications is introduced and the analysis of the remote attestation scenario for the TPM is explained in more detail.

Thursday 12th June:
Speaker: Matt Robshaw (Orange-France Telecom)
Title: Lightweight Cryptography
Abstract: The physical limitations of tiny devices such as RFID tags are so demanding that many standard cryptographic algorithms cannot be used. However, several new designs have been proposed in recent years, and in this presentation we survey the current state of the art of lightweight cryptographic algorithms.

Thursday 19th June:
No seminar

Thursday 26th June:
Speaker: Christian Rechberger (TU Graz)

Title: Advances in Hash Cryptanalysis
Abstract: Hash functions are the Swiss army knife for cryptographers. Password protection, digital signatures (also in a potential post-quantum period) are applications where they surface outside the cryptographic community. Not only are almost all popular hash functions based on the same design principle, it also turned out that designers were not conservative enough. Spectacular practical attacks (e.g. on MD5) were the result in recent years, and standardization organisations look for replacements.

The ubiquitously used SHA-1 exhibits a higher resistance against shortcut collision search attacks. Still, to motivate the shift away from SHA-1, we found a new shortcut attack which is estimated to be around a million times faster than generic attacks. The workfactor is still very high and hence we started a distributed computing project to find the first SHA-1 collision.

Many applications of hash functions do not require collision resistance but rely on properties that are generally assumed to be much harder to violate (like resistance against inversion attacks). Nevertheless, some of our very recent results indicate that also here, we might see a development similar to collision attacks.

The programme for the first semester of the 2007/2008 academic year was as follows:

Thursday 4th October:
Speaker: Takeshi Okamoto (Visiting Researcher, RHUL, and University of Tsukuba, Japan)
Title: 1-out-of-n Signature and its Application
Abstract: 1-out-of-n signature convinces a verifier that a message is singed by one-of-n possible signers without any information related to the actual signer. Recently, Boneh et al. proposed a pairing-based broadcast encryption scheme. In our study, we give the converting technique from broadcast encryption to 1-out-of-n signature. Moreover, a practical protocol of 1-out-of-n signature is also proposed. One of the remarkable advantages in our scheme is that the size of signature does not depend on n. We can construct 1-out-of-n signature with 580 bits length although the key size satisfies the current security requirement.

Thursday 11th October:
Speaker: Long Nguyen (University of Oxford)
Title: Authentication protocols based on human interaction in security pervasive computing
Abstract: A big challenge in pervasive computing is to establish secure communication over the Dolev-Yao network without any initial knowledge or a Public Key Infrastructure. An approach studied by a number of researchers is to build security though human work creating a low-bandwidth empirical (or authentication) channel where the transmitted information is authentic and cannot be faked or modified. An example is conversation between the users of systems. In this talk, we give a brief analytical survey of authentication protocols of this type as well as concentrating on our contribution to this area. These are our proposed group protocols and a new cryptographic primitive termed a Digest function that uniformly and efficiently digests/compresses many kilobytes of information into a short string output (perhaps 16 bits). We start with non-interactive schemes, for example: the one proposed by Gehrmann, Mitchell and Nyberg, and point out that it does not optimise the human work, and then present our improved version of the scheme. We then move on to analyse a number of strategies used to build interactive pair-wise and group protocols that minimise the human work relative to the amount of security obtained as well as optimising the computation processing. Many of the protocols are based on the human comparison of a single short

authentication string, transmitted over the empirical channel that is the output of the Digest function. We finish the talk with our proposed implementation of the Digest function, based on matrix multiplication and pseudo-random number generation, as well as some theoretical results about the digest.

Thursday 18th October:
Speaker: Maura Paterson (ISG, RHUL)
Title: A Geometric View of Cryptographic Equation Solving
Abstract: In this talk we consider the geometric properties of the XL algorithm used in cryptology for solving systems of multivariate polynomial equations. We provide a geometrically invariant generalisation, which we term the GeometricXL algorithm. We show how this algorithm (and, consequently, the original XL algorithm) relates to the problem of finding a matrix of low rank in the linear span of a collection of matrices, a problem sometimes known as the MinRank problem. Furthermore, we demonstrate that the GeometricXL algorithm can solve certain equation systems that are not easily soluble by the XL algorithm or by Groebner basis methods.

Monday 22nd October at 12pm:
Speaker: Wenbo Mao (EMC)
Title: Daoli - Grid security with behavior conformity from Trusted Computing (TC) protected virtualization
Abstract: A grid builds a virtual organization (VO) of unbounded computational and storage capacity by pooling heterogeneous resources from real organizations (lessors). Currently such grids are not commercially seriously adopted yet. Ideally, commercial enterprises, like resource-abundant-and-under-utilized financial institutions, should ‘‘go for grid,’’ i.e., become lessors. Inadequate grid security currently prevents commercial organizations from being lessors. A missing security service is behavior conformity: VO (lessee's) code mustn’t damage the lessor; conversely, the lessor mustn’t compromise lessee's proprietary information.

Project Daoli strengthens grid security by adding behavior conformity in two layers of virtualization with the software stack to be protected by a Trusted Platform Module (TPM). At the OS layer, a highly-privileged hypervisor for memory arbitration will be hashed in TPM for integrity protection. Above OSes, a grid middleware virtualizes platforms so that a unique piece of VO code can run across a heterogeneous environment of lessors. This VO code is for policy enforcement and can be propagated to execute in remote platforms with cryptographic credentials being migrated from one TPM to another along the leased platforms.

Thursday 25th October:
Speaker: Gerhard Hanke (Smart Card Centre, ISG, RHUL)
Title: Distance-Bounding: Proof of Proximity
Abstract: Location, or proximity, provides a measure of trust with regards to security. Distance-bounding protocols determine an upper bound for the physical distance between two communicating parties without assistance from a third party. This cryptographically verified distance can then be used as a secure measure of proximity. To achieve a reliable distance bound the protocol must be integrated into the physical layer of the communication channel. This means that the security of these protocols not only depends on the cryptographic protocol itself but also on the practical implementation and the physical attributes of the communication channel. This talk gives a brief overview of distance-

bounding protocols, the attacks they aim to prevent and the importance of implementing a suitable communication channel.

Thursday 1st November:
Speaker: Jason Crampton (ISG, RHUL)
Title: Cryptographically-Enforced Hierarchical Access Control with Multiple Keys
Abstract: Hierarchical access control policies, in which users and objects are associated with nodes in a hierarchy, can be enforced using cryptographic mechanisms. Protected data is encrypted and authorized users are given the appropriate keys. Lazy re-encryption techniques and temporal hierarchical access control policies require that multiple keys may be associated with a node in the hierarchy. In this paper, we introduce the notion of a multi-key assignment scheme to address this requirement. We define bounded, unbounded, synchronous, and asynchronous schemes. We demonstrate that bounded, synchronous schemes provide an alternative to temporal key assignment schemes in the literature, and that unbounded asynchronous schemes provide the desired support for lazy re-encryption.

Thursday 8th November:
Speaker: Lizzie Coles-Kemp (ISG, RHUL)
Title: Adaptable security management structures for the management of dynamic, complex organisations
Abstract: Information security management structures are typically regarded as hierarchical and top down and, whilst this structure is suited to static, bureaucratic organisations, rigid management structures are often fragile and slow to respond when an organisation is both complex and structurally dynamic. Such complex organisations typically use dynamic and adaptable technology and require the same properties from their security management structures. The recursive property of the Viable System Model can be applied to security where each information security management system calls a sub-system down to the level of a single organisational cell. This enables security management structures to absorb and respond to context complexity and to rapidly react to change. This presentation presents research which compares the hierarchical and recursive approaches to security management, the effect each approach has both on security management process design and on the ability to manage technical as well as organisational stakeholders.

Thursday 15th November:
Speaker: Stephane Lo Presti (ISG, RHUL)
Title: A Tree of Trust rooted in Extended Trusted Computing
Abstract: Trusted Computing and its associated technologies are continuing to gain momentum in the computing world. We present the result of the study the structure of the concept of trust in the largest sense in the Extended Trusted Computing paradigm, which combines Trusted Computing and Virtualisation technologies. We extend the notion of a chain of trust into a Tree of Trust (ToT) concept and notation in order to represent the Extended Trusted Computing platform's trust structure. A ToT is a tree whose nodes represent the various platform components, from the hardware TPM up to the running applications, annotated with trust and security statements. The ToT can be used to better understand the trust that one should put into the platform, or even to reorganise the platform according to certain constraints.

Thursday 22nd November:
Speaker: Frederic Stumpf (TU Darmstadt)
Title: Trust, Security and Privacy in VANETs - A Multilayered Security Architecture for

Car2Car-Communication
Abstract: As we move into an era of networked systems, vehicles are also being equipped with wireless communication technologies. Based on these abilities, different vehicles are able to exchange information related to traffic safety and thus increase traffic safety and efficiency. A particular vehicle could for example be warned about danger situations that have been detected by sensors of another vehicle. In this context, this talk considers multi-hop messages, e.g., Vehicle based Road Condition Warning and single hop messages, e.g., Emergency Electronic Brake Lights. However, the introduction of safety message raises severe security challenges. Since these messages influence the behaviour of critical components, a misuse of safety messages can result in serious accidents.

These safety messages require trusted software components to ensure that a particular safety message is based on real events and not injected from a malicious vehicle. Additionally, it is also necessary to have a mechanism that can isolate misbehaving vehicles from the network. Compounding this problem is that a vehicle owner could transfer identification data to other vehicles, which undermines the possibility to clearly identify and isolate misbehaving vehicles.

This talk presents a multi-layered security protocol that enables a vehicle to take part in Inter-vehicle communication for safety information, while satisfying the above mentioned requirements. The solution is based on two main schemes: Attestation of virtualized system components and secure revocable anonymous authenticated communication.

The Inter-vehicle communication protocol uses methods to increase unlinkability of distinct messages. The certification protocol utilises revocable blinded signatures and shared secrets to provide an adjustable tradeoff between authenticity and privacy. Tracing requests by the traffic authorities are fulfilled by mapping certificates to identities of vehicle owners by shared secret interpolation. This process enforces the many-eye principle to protect the user's privacy while ensuring that the traffic authorities are able to trace and exclude rogue vehicles.

Thursday 29th November:
Speaker: Michel Abdalla (ENS and CNRS, France)
Title: Robust Encryption
Abstract: Motivated by applications to auctions, searchable encryption, and anonymous wireless communication, we provide a provable-security treatment of the folklore notion of a ``robust'' encryption scheme, namely one where the decryption algorithm rejects when the ``wrong'' secret key is used. We provide formal definitions of robustness under chosen-plaintext and chosen-ciphertext attacks. We find that contrary to what seems intuitive, robustness ---at least in combination with privacy and anonymity as required by applications--- is actually rarely, if ever, present and obvious ways to confer it fail. We however provide general ways to efficiently confer robustness without sacrificing other security properties, both for public key and identity-based encryption. We also examine the robustness of well-known encryption schemes. Joint work with Mihir Bellare, Chanathip Namprempre and Gregory Neven.

Thursday 6th December:
Speaker: Hoon Wei Lim (ISG, RHUL)
Title: Multi-key hierarchical signatures
Abstract: We motivate and investigate a new cryptographic primitive that we call multi-key hierarchical identity-based signatures (multi-key HIBS). Using this primitive, a user is able to

prove possession of a set of identity-based private keys associated with nodes at arbitrary levels of a hierarchy when signing a message. Our primitive is related to, but distinct from, the notions of identity-based multi-signatures and aggregate signatures. We develop a security model for multi-key HIBS. We then present and prove secure an efficient multi-key HIBS scheme that is based on the Gentry-Silverberg hierarchical identity-based signature scheme.

Thursday 13th December:
Seminar cancelled

Previous talks in 2007:

- **Date:**Tuesday, 11th Sep

Speaker: Danny De Cock (K.U. Leuven)

Title: Overview of the Belgian Identity Management
Infrastructure and eID Cards Architecture

Abstract: In this presentation, we will give an overview of
the main components of the eGovernment systems in Belgium. This includes the
milestones of the Belgian eID card project, the eID card's issuing process, and
examples of their use.

After the presentation, you will know details about:

- the eID card content (key pairs, certificates, identity data, etc.)
- the certificate hierarchy and details on the individual
certificates (citizen, CA, government, etc.)
- certificate revocation lists management
- typical use scenarios to generate signatures, verify signatures,
key pair properties, certificate (chain) validation procedures, etc.
- issues with respect to long-term validity of digital signatures
relying on certificates which may have been revoked at some moment.

- **Date:** Monday, 3rd September

Speaker: Nils Aschenbruck (Communication Systems Group at the
University of Bonn)

Title: Modelling Mobility in Disaster Area Scenarios

Abstract: When creating a scenario for performance evaluation
of a communication system, modelling the mobility is an important task, since
the results of the evaluation strongly depend on the model used. Typical
assumptions of many models are uniform selection of destinations, nodes are
allowed to move over the whole simulation area, and nodes are part of the
network all the time (are not switched off and do not leave the network).

An analysis of tactical issues in civil protection provides characteristics influencing network performance in public safety communication networks like heterogeneous area-based movement, obstacles, and joining/leaving of nodes. These characteristics differ significantly from the typical assumptions. The talk will present a new model that realistically represents the movements in a disaster area scenario. The new model shows specific characteristics like heterogeneous node density. These characteristics do also have specific impact on the results of simulative network performance analysis. Finally, future work is presented focusing on performance evaluation of several intrusion detection detectors for tactical mobile networks.

- **Date:** Tuesday, 21st Aug

Speaker: Ben Smith (ISG, RHUL)

Title: Isogenies and the DLP on Jacobians of genus three curves

Abstract: In this talk, we describe the use of isogenies (a special type of homomorphism) to reduce DLPs on Jacobians of hyperelliptic genus 3 curves to DLPs on non-hyperelliptic Jacobians, which are generally regarded as being cryptographically weaker. This exposes hyperelliptic Jacobians to the faster index-calculus algorithms available for non-hyperelliptic Jacobians, reducing the time required to solve DLPs from $\softO(q^{4/3})$ to $\softO(q)$. We will give an algorithm which quickly constructs an explicit reduction for around 17% of (randomly chosen) hyperelliptic genus three curves. We conclude that the DLP on hyperelliptic genus three Jacobians is not intrinsically harder than the DLP in the non-hyperelliptic case.

- **Date:** Tuesday, 31st July

Speaker: Bruce Beckles (University of Cambridge)

Title: The PKI don't work: Using PKI appropriately in grid environments

Abstract: In this talk I shall outline some of the problems encountered with the existing public key infrastructure (PKI) used in most current computational grid environments. The nature of these problems means that PKI is unsuitable for use by end-users, and, if it is to be used in the grid environment, end-users must have minimal direct interaction - in fact, preferably no interaction - with the PKI mechanisms. I will discuss two approaches to "removing PKI from the end-user's experience of the grid environment" currently being explored by a research project with which I am associated. These approaches have the potential to significantly improve the usability of the security infrastructure of the grid environment, thus removing (or lowering) one of the major hurdles faced by new grid users, as well as substantially improving the security of these environments.

- **Date:** Tuesday, 24th July

Speaker: Jens Jensen (Rutherford Appleton Laboratories)

Title: e-Science and Grid Security

Abstract: The Grid ties together heterogeneous and distributed computing and storage resources on a global scale. With its growth in size and popularity comes security issues, ranging from low level machine security to managing dynamic virtual organisations, and from practical implementations to security research. This talk introduces introduces Grid security with an overview of this range, and will then look at recent developments and open issues. The talk will be of interest to anyone with an interest in Grid security and applied security research.

- **Date:** Tuesday, 19th June

Speaker: James Birkett (ISG, RHUL)

Title: Identity Based Key Encapsulation with Wildcards

Abstract: We propose new instantiations of chosen-ciphertext secure identity-based encryption schemes with wildcards (WIBE). Our schemes outperform all existing alternatives in terms of efficiency as well as security. We achieve these results by extending the hybrid encryption (KEM-DEM) framework to the case of WIBE schemes. We propose and prove secure one generic construction in the random oracle model, and one direct construction in the standard model.

- **Date:** Tuesday, 5th June

Speaker: Matt Barrett

Title: Towards an Open Trusted Computing Framework

Abstract: I will give a brief introduction to trusted computing, for those not familiar. I will discuss my master's thesis, which was concerned with open trusted computing frameworks. An analysis of two secure operating system frameworks built upon the Trusted Computing Group's Trusted Platform Module will be given, and the security implications of the respective design decisions discussed. The complexity and difficulty in providing assured computation, while keeping the flexibility of general purposes computers, is highlighted.

I will discuss in some detail a novel insertion attack against certain trusted computing frameworks built upon the TCG's TPM. Our insertion attack makes use of a vulnerability that arises due to the architecture of the TPM itself, and was published at COMPSAC 2006.

- **Date:** Tuesday, 29th May

Speaker: Kenny Paterson (ISG, RHUL)

Title: Attacking the IPsec Standards in Encryption-only
Configurations

Abstract: We describe new attacks which break any RFC-compliant implementation of IPsec making use of encryption-only ESP in tunnel mode. The new attacks are both efficient and realistic: they are ciphertext-only and need only the capability to eavesdrop on ESP-encrypted traffic and to inject traffic into the network. We report on our experiences in applying the attacks to a variety of implementations of IPsec. Joint work with Jean Paul Degabriele (currently with Hewlett-Packard Labs).

- **Date:** Tuesday, 15th May

Speaker: Imad Abbadi (ISG, RHUL)

Title: Digital Rights Management using a Mobile Phone

Abstract: This paper focuses on the problem of preventing illegal copying of digital assets without jeopardising the right of legitimate licence holders to transfer content between their own devices, which make up a domain. Our novel idea involves the use of a domain-specific mobile phone and the mobile phone network operator to authenticate the domain owner before devices can join a domain. This binds devices in a domain to a single owner, that, in turn, enables the binding of domain licences to the domain owner. In addition, the way in which we control domain membership, and the use of the domain-specific mobile phone that enables a domain owner to add devices wherever he/she is physically present, ensures that devices joining the domain are in physical proximity to the mobile phone, preventing illicit content proliferation.

- **Date:** Thursday, 22nd March

Speaker: Søren Thomsen (visiting ISG, RHUL)

Title: Grindahl - a family of hash functions

Abstract: In this paper we propose the Grindahl family of hash functions, which is based on components of the Rijndael algorithm. To make collision search sufficiently difficult, this design has the important feature that no low-weight characteristics form collisions, and at the same time it limits access to the state. We also propose two instances of the Grindahl hash family, Grindahl-256 and Grindahl-512 with claimed security levels with respect to collision, preimage and second preimage attacks of 2^{128} and 2^{256}, respectively. Both proposals have lower memory requirements than other hash functions at comparable speeds and security levels.

- **Date:** Tuesday, 20th March

Speaker: Hoon Wei Lim (ISG, RHUL)

Title: A Certificate-free Grid Security Infrastructure
Supporting Password-based User Authentication

Abstract: Password-based authentication is still the most widely used authentication mechanism, largely because of the ease with which it can be understood by end users and implemented. We propose a security infrastructure for grid applications, in which users are authenticated using passwords. Our infrastructure allows users to perform single sign-on based only on passwords, without requiring a public key infrastructure. Nevertheless, our infrastructure supports essential grid security services, such as mutual authentication and delegation, using public key cryptographic techniques. Moreover, hosting servers in our infrastructure are not required to have public key certificates, meaning mutual authentication and delegation of proxy credentials can be performed in a lightweight and efficient manner.

- **Date:** Tuesday, 13th March

Speaker: Sean Murphy (ISG, RHUL)

Title: Forgery Attacks on HMAC

Abstract: HMAC is a message authentication code based on an n-bit hash function. The generic forgery attack attack on HMAC requires 2^{n/2} message-MAC pairs. We describe a attack against a generic HMAC requiring less than 2^{n/2} message-MAC pairs.

- **Date:** Tuesday, 6th March

Speaker: Carlos Cid (ISG, RHUL)

Title: An Analysis of the Hermes8 Stream Ciphers

Abstract: Hermes8 is one of the 34 stream ciphers submitted to the ECRYPT Stream Cipher Project (eSTREAM). In this talk we will present an analysis of the Hermes8 stream ciphers. In particular, we show an attack on the latest version of the cipher (Hermes8F), which requires very few known keystream bytes and recovers the cipher secret key in less than a second on a normal PC. Furthermore, we make some remarks on the cipher's key schedule and discuss some properties of ciphers with similar algebraic structure to Hermes8.

This is a joint work with Steve Babbage, Norbert Pramstaller and Haavard Raddum, and parts of it were presented at the SASC 2007 workshop in Bochum.

- **Date:** Tuesday, 27th Feb

Speaker: Adrian Leung (ISG, RHUL)

Title: Ninja : Non Identity Based, Privacy Preserving
Authentication for Ubiquitous Environments

Abstract: Most of today's authentication schemes are based on authenticating the identity of a principal in one way or another. This method of authentication is commonly known as entity authentication. In emerging computing paradigms which are highly dynamic and mobile in nature, such as a ubiquitous environment, entity authentication alone may not be sufficient or even appropriate, especially if a principal's privacy is to be protected. In order to preserve the privacy of a principal, other attributes (such as location or trustworthiness) of the principal may need to be authenticated to a verifier. In this paper, in the context of a mobile ubiquitous environment, we propose Ninja: a non identity based authentication scheme, whereby the trustworthiness of a user's device is authenticated anonymously to a remote Service Provider (verifier), during the service discovery process. We show how this can be achieved using the functionalities of Trusted Computing.

- **Date:** Wednesday, 21st Feb

Speaker: Patrick Baier

Title: Special purpose hardware for integer factorisation

Abstract: I would like to discuss the use of reconfigurable hardware (FPGAs) to speed up some of the sub-algorithms of the number field sieve, in particular the relation collection step. I intend to focus on the implementation of Lenstra's Elliptic Curve Method in hardware, which can be used as an efficient smoothness test and a tool for factoring the sieving reports. A significant improvement over microprocessors can be achieved in terms of performance to cost.

- **Date:** Tuesday, 20th Feb

Speaker: Qiang Tang (ISG, RHUL, and ENS Paris)

Title: Biometric cryptosystems: issues, challenges, and possible solutions

Abstract: Biometrics, such as fingerprint and iris, have been used to a higher level of security in order to cope with the increasing demand for reliable and highly-usable information security systems, because they have many advantages over cryptographic credentials. However, in practice, there are some obstacles (or concerns) in a wide adoption of biometrics. Biometric features are volatile over the time, and they are also sensitive data. In this talk, we have a review of the security issues and challenges faced by biometric cryptosystems. We then highlight some possible solutions in identification, authentication, and biometric-based key release systems.

- **Date:** Tuesday, 13th Feb

Speaker: Jiqiang Lu (ISG, RHUL)

Title: Related-key rectangle attack on 42-round SHACAL-2

Abstract: Based on the compression function of the hash function standard SHA-256, SHACAL-2 is a 64-round block cipher with a 256-bit block size and a variable length key of up to 512 bits. In this paper, we present a related-key rectangle attack on 42-round SHACAL-2. This is the best currently known attack on SHACAL-2 in terms of the numbers of attacked rounds.

- **Date:** Friday, 9th Feb

Speaker: David Chadwick (University of Kent)

Title: Building a Modular Authorisation Infrastructure

Abstract: Authorization infrastructures manage privileges and render access control decisions, allowing applications to adjust their behavior according to the privileges allocated to users. This talk describes the conceptual authorisation, access control, and trust models that are required for a modular authorisation infrastructure. I will then say how we have implemented this model in Open PERMIS (www.openpermis.org). PERMIS has the novel concept of a credential validation service, which verifies a user's credentials prior to access control decision making and enables the distributed management of credentials. Details of the design and the implementation of PERMIS are presented along with details of its integration with Globus Toolkit, Shibboleth and GridShib. A comparison of PERMIS with other authorization and access control implementations is given, along with our plans for the future.

- **Date:** Tuesday, 6th Feb

Speaker: Po Yau (ISG, RHUL)

Title: Secure packet delivery reporting in ad hoc networks

Abstract: Selfish nodes pose a threat to the availability of communications in mobile ad hoc networks. Many schemes proposed to deal with this threat rely on passive acknowledgements, a mechanism that relies on the properties of wireless communication. We will show that inherent problems exist when using passive acknowledgements to detect selfish or non-forwarding behaviour. We propose an efficient protocol that uses explicit network layer acknowledgements to provide a means of detecting non-forwarding nodes with stronger assurances.

- **23 Jan**: "Solving Systems of Polynomial Equations with a SAT-Solver", Greg Bard.
Abstract: Solving a system of polynomial equations over a finite field is a basic problem at the heart of algebraic cryptanalysis. Unfortunately, it is NP-Complete. On the other hand, the CNF-SAT problem is also NP-Complete, and all NP-Complete problems are equivalent to each other. In recent years, there have been great strides in the development of general purpose "SAT-Solvers" which quickly solve SAT problems of large size.

Converting a system of polynomials to a CNF-SAT problem results in an exponentially long logical sentence if done naively. However, simple tricks can be used to make the logical sentence linear in length compared to the original polynomial system, and the conversion runs in LOGSPACE not PSPACE. Since SAT-solvers are also LOGSPACE, this method of polynomial system solving requires very little memory.

In the end, this means that with a suitable converter, much larger polynomial systems can now be solved than was previously thought possible. In fact, it was precisely this method that allowed algebraic cryptanalysis of the Data Encryption Standard out to six rounds, an example which I will describe in extended detail.

Previous talks presented in 2006:

- **12 Dec**: "Experiences Developing Secure, User-oriented Grid Infrastructures at the National e-Science Centre (NeSC)", Richard Sinnott (Glasgow).
  Abstract: Security underpins Grids and e-Research.
  Without a robust, reliable and simple Grid security infrastructure combined with commonly accepted security practices, large portions of the research community and wider industry will not engage. The predominant way in which security is currently addressed in the Grid community is through Public Key Infrastructures (PKI) based upon X.509 certificates to support authentication. Whilst PKIs address user identity issues, authentication does not provide fine grained control over what users are allowed to do on remote resources (authorisation). Users are also uncomfortable with the whole process of obtaining and using X.509 certificates. In this talk we outline problems with existing Grid security models and outline how Shibboleth technology offers a new paradigm which can simplify the user experience of interacting with Grid infrastructures. We show that when combined with a suitable authorisation infrastructure, Shibboleth can improve the overall security needed for multi-discipline, multi-organisational e-Research. We demonstrate this through practical examples of different security focused e-Science projects being conducted at the National e-Science Centre (NeSC) at the University of Glasgow. We believe that this model will become the de facto way in which future e-Research resources are accessed by a wide variety of researchers, not just the existing (and small) Grid-savvy community.
- **5 Dec**: "Steganography, Steganalysis, and Capacity", Andrew Ker (Oxford).
  Abstract: Steganography is a branch of information
  hiding aiming to transmit a message concealed in some digital media object, so that its presence cannot be deduced by a third party. In the talk I will propose a new model for steganography and the competing aim of steganalysis, in which we allow the payload to be split between multiple cover objects. This model sheds light on the fundamental question of the capacity of covert steganographic channels, which has resisted analysis until now. Given the new model, and some fairly general assumptions about the nature of steganalysis in single objects, we can show that the capacity of a batch of N objects is asymptotically of the order of the square root of N.

- **28 Nov**: "Differential and Rectangle Attacks on Reduced-Round SHACAL-1", Jiqiang Lu.

  Abstract: SHACAL-1 is an 80-round block cipher with a 160-bit block size and a key of up to 512 bits, which is based on the well known hash function standard SHA-1. In this paper, we mount rectangle attacks on the first 51 rounds and a series of inner 52 rounds of SHACAL-1, and also mount differential attacks on the first 49 rounds and a series of inner 55 rounds of SHACAL-1. These are the best currently known cryptanalytic results on SHACAL-1 in a single key attack scenario.
- **21 Nov**: "A Web Services Shopping Mall for Mobile Users", Kalid Elmufti (City University).
  Abstract: We present a platform for the direct consumption of web services by a Mobile Station. We give an architectural solution where Mobile Operators play the role of Trusted Third Parties supplying service credentials that allow a co-located 3GPP Network Application Function and Liberty-enabled Identity Provider entity to implement a controlled Shopping Mall service to Mobile Stations from multiple trust domains. We are using 3GPP Generic Authentication Architecture (GAA) and SSO to develop a mobile Web services solution.
- **24 Oct**: "The Fourth Game Hop: A More Efficient Proof Of Waters Encryption", Alex Dent.

  Abstract: Game hopping has become a popular tool to simplify security proofs. It easily allows a researcher to prove the security of a complex algorithm one step at a time. The literature describes three types of game hop: bridging steps, transitions based on (small) error events, and transitions based on indistinguishability. In this talk, we present a new, fourth type of game hop (transitions based on large events) and use it to re-prove the security of the Waters based encryption scheme in a more efficient way.
- **Friday, 29 Sep**: "Pairing Based Threshold Cryptography, Improving on Libert-Quisquater and Baek-Zheng", Yvo Desmedt (University College London).

  Abstract:

  We apply techniques from secret sharing and threshold decryption to show how to properly design an ID-based threshold system in which one assumes no trust in any party.
  In our scheme:

  - We avoid that any single machine ever knew the master secret s of the trusted authority (TA). Instead only shares of it will be known by parties of the distributed TA and it can be seen as a virtual key.
  - The threshold t_{TA} and the number of shareholders n_{TA} used by the distributed TA do not need to be identical to the ones used by user ID. Moreover, each user ID can use its own values for the threshold t_{i} and the number of parties n_{i} that will acquire shares.

  - No single machine will ever know the secret key of the user -- this means no single machine in the distributed TA and no shareholder of the user ID.

  Like Baek and Zheng suggest, such a scheme can be turned into a mediated system.
  This is joint work with Tanja Lange and was presented at Financial Cryptography 2006 (February, not yet published).

- **29 Aug**: "Universal Designated Verifier Signatures Without Random Oracles or Non-Black Box Assumptions", Benoit Libert.

  Abstract: Universal designated verifier signatures (UDVS) were introduced in 2003 by Steinfeld et al. to allow signature holders to monitor the verification of a given signature in the sense that any plain signature can be publicly turned into a signature which is only verifiable by some specific designated verifier. Privacy issues, like non-dissemination of digital certificates, are the main motivations to study such primitives. In this work, we propose two efficient UDVS schemes which are secure (in terms of unforgeability and anonymity) in the standard model (i.e. without random oracles). Their security relies on algorithmic assumptions which are more classical than assumptions involved in the two only known UDVS schemes in standard model to date. The latter schemes, put forth by Zhang et al. in 2005 and Vergnaud in 2006, rely on the Strong Diffie-Hellman assumption and the strange-looking ``knowledge of exponent assumption'' (KEA). Our schemes are obtained from Waters's signature and they do not need the KEA assumption. They are also the first random oracle-free constructions with the anonymity property.

  joint work with F. Laguillaumie and J.-J. Quisquater

- **14 Aug**: "On the Evolution of Adversary Models in Security Protocols - from the Beginning to Sensor Networks", Virgil D. Gligor, (University of Maryland).
  Abstract: Invariably, new technologies introduce new vulnerabilities which often enable new attacks by increasingly potent adversaries. Yet new systems are more adept at handling well-known attacks by old adversaries than anticipating new ones. Our adversary models seem to be perpetually out of date: often they do not capture adversary attacks and sometimes they address attacks rendered impractical by new technologies.

  In this talk, I provide a brief overview of adversary models beginning with those required by program and data sharing technologies ('60-'70s), continuing with those required by computer communication and networking technologies ('70s-'90s), and ending with those required by and sensor network technologies ('00s ->). I argue that sensor, ad-hoc, and mesh networks require new models, different from those in common use, namely those of the Dolev-Yao and Byzantine adversaries. I illustrate this with adversaries that attack perfectly sensible and otherwise correct protocols of sensor networks. These attacks cannot be countered with traditional security protocols using end-to-end design arguments and require emergent security properties as countermeasures.

- **15 Aug**: "A Challenging But Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL", Greg Bard.
  Abstract: The purpose of this paper is to explain a cryptanalytic vulnerability in SSL 3.0 and TLS 1.0, which can be exploited to recover plaintexts of low entropy with probability approaching one. The method is an example of a blockwise-adaptive chosen-plaintext attack, exploiting the insecurity of the CBC encryption mode in that model. An example of a low entropy plaintext would be a selection from a list of 2--1000 items, such as a stock ticker or city name. While the vulnerability has been closed in later editions of the TLS protocol, this paper hopes to motivate system administrators that use SSL to switch to TLS 1.1 or later; demonstrate that the blockwise-adaptive chosen-plaintext model is not sterile and purely academic; highlight the importance of the location of secret data among block boundaries; provide an example of how an attacker can achieve t