LMS Computer Science Colloquium 2018: Agenda

Mathematics of Security

Wednesday 13 November 2019, 10:00am - 4:00pm

London Mathematical Society, De Morgan House, London WC1B 4HS

10:00–10:30	Registration and coffee
10:30–11:30	David Galindo (Birmingham) *Security Models and Designs from E-Voting to Blockchain*
11:30–12:30	Alexei Lisitsa (Liverpool) *Formal Modelling of Smart Contracts Languages, Their Expressive Power and Verification*
12:30–13:30	Lunch break
13:30–14:30	Christophe Petit (Birmingham) *Rubik's for cryptographers: Babai's conjecture, hash functions and quantum gates*
14:30–15:30	Delaram Kahrobaei (York) *Interactions between Group Theory, Cyber Security, Artificial Intelligence, and Quantum Computation*
15:30–16:00	Refreshments

LONDON MATHEMATICAL SOCIETY
EST. 1865

Speaker abstracts and biographies

David Galindo (Birmingham)
Security Models and Designs from E-Voting to Blockchain

Abstract: This talk addresses two fascinating and polarising topics from the point of view of computer security: electronic voting and blockchain. In the first part, an overview of cryptographic definitions for security and privacy for electronic voting is provided. In doing so, both canonical as well as practical designs conjectured to meet those definitions will be presented. Next, and perhaps surprisingly, similarities with blockchain cryptographic definitions and protocols will be highlighted.

David Galindo is a Senior Lecturer in Computer Security at the School of Computer Science at the University of Birmingham with 15 years of experience in applied cryptography research. He is a member of the University's Centre for Cyber Security and Privacy. He is also Lead Cryptographer in Cambridge-based AI and digital economics start-up Fetch.ai. His work has been published in top academic venues in computer security and has been deployed by governments around the globe. David's research is in the interplay of mathematics and computer science, more precisely in cryptographic protocols for security, and it is usually motivated by practical problems.

Alexei Lisitsa (Liverpool)
Formal Modelling of Smart Contracts Languages, Their Expressive Power and Verification

Abstract: Smart Contracts have become very popular recently. In this talk, I will address the questions of formal modelling of smart contracts languages, their expressive power and automated safety and security verification. I will argue that common reference to Turing completeness of the contract languages is not always an adequate measure of their fitness, as the main purpose of a contract is to demonstrate a behaviour rather than compute a function. As the main modelling formalism, I will introduce BitML, a high-level and declarative formal language proposed recently by M. Bartoletti and R. Zunino for contracts specification and will discuss also modelling by First-Order Logic (FOL) and Abstract State Machines (ASM). I will present some results and open questions on the expressive power of BitML and its extensions. One of the advantages of the formal approach is an opportunity to formulate and address rigorously the questions of impossibility or infeasibility of smart contracts. From that perspective, I will discuss a formal reconstruction of the recent claim of the infeasibility of so-called smart Obama-Trump contract (Y. Wang and Q.M. Malluhi, CACM May 2019).

Alexei Lisitsa is a Lecturer in the Department of Computer Science at Liverpool University and Head of the Verification Group, part of the Artificial Intelligence section in the Department of Computer Science. His research interests are in Formal Methods, Verification, Applied Automated Reasoning, Applied Machine Learning and Security.

Christophe Petit (Birmingham)
Rubik's for cryptographers: Babai's conjecture, hash functions and quantum gates

Abstract: Hard mathematical problems are at the core of security arguments in cryptography. In this talk, I will discuss mathematical generalizations of the famous Rubik's cube puzzle. I will relate them to a conjecture of Babai on the diameter of finite simple groups, to the security of particular cryptographic constructions, to the design of efficient quantum circuits, and more.

Christophe Petit is a Senior Lecturer at the University of Birmingham's School of Computer Science, and a member of the Security and Privacy research group. He is also actively involved within Oxford's Mathematical Institute, where he helped found the Cryptography group. He teaches the Secure Programming and part of the Advanced Cryptography module at Birmingham, which are both of the Masters in Cybersecurity. In the past he taught an Advanced Cryptography reading course for the Masters in Mathematics and Foundations of Computer Science at Oxford.

Delaram Kahrobaei (York)

Interactions between Group Theory, Cyber Security, Artificial Intelligence, and Quantum Computation

Abstract: In this talk, I explore how group theory playing a crucial role in cyber security and quantum computation. At the same time, how computer science for example machine learning algorithms and computational complexity could help group theorists so tackle their open problems, as such this could help with cryptanalysis of the proposed primitives.

Symmetry is present in all forms in the natural and biological structures as well as man-made environments. Computational symmetry applies group-theory to create algorithms that model and analyze symmetry in real data set. The use of symmetry groups in optimizing the formulation of signal processing and machine learning algorithms can greatly enhance the impact of these algorithms in many fields of science and engineering where highly complex symmetries exist.

At the same time, Machine Learning techniques could help with solving long standing group theoretic problems. For example, in the paper [J. Gryak (University of Michigan, Data Science Institute), R. Haralick (The City University of New York, the prize recipient of International Association for Pattern Recognition), D. Kahrobaei, Solving the Conjugacy Decision Problem via Machine Learning, Experimental Mathematics, Taylor & Francis (2019)] the authors use machine learning techniques to solve the conjugacy decision problem in a variety of groups. Beyond their utilitarian worth, the developed methods provide the computational group theorist a new digital "sketchpad" with which one can explore the structure of groups and other algebraic objects, and perhaps yielding heretofore unknown mathematical relationships.

Graph theoretic problems have been of interest of theoretical computer scientists for many years, especially the computational complexity problems for such algorithmic problems. Such studies have been fruitful for one of the millennium problems (P vs NP) of the Clay Math Institute. Since graph groups are uniquely defined by a finite simplicial graph and vice versa, it is clear that there is a natural connection between algorithmic graph theoretic problems and group theoretic problems for graph groups. Since the graph theoretic problems have been of central importance in complexity theory, it is natural to consider some of these graph theoretic problems via their equivalent formulation as group theoretic problems about graph groups. The theme of the paper [Algorithmic problems in right-angled Artin groups: Complexity and applications, R. Flores, D. Kahrobaei, T. Koberda, J. of Algebra, Elsevier 2019.] is to convert graph theoretic problems for finite graphs into group theoretic ones for graph groups (a.k.a. right-angled Artin) groups, and to investigate the graph theory algebraically. In doing so, new approaches to resolving problems in complexity theory become apparent. The authors are primarily motivated by the fact that some of these group theoretic problems can be used for cryptographic purposes, such as authentication schemes, secret sharing schemes, and key exchange problems.

In the past couple of decades many groups have been proposed for cryptography, for instance: polycyclic groups for public-key exchanges, digital signatures, secret sharing schemes (Eick, Kahrobaei), hyperbolic groups for private key encryption (Chatterji-Kahrobaei), p-groups for multilinear maps (Kahrobaei, Tortora, Tota) among others.

Most of the current cryptosystems are based on number theoretic problems such discrete logarithm problem (DLP) for example Diffie-Hellman key-exchange. Recently there has been some natural connections between algorithmic number theoretic and algorithmic group theoretic problems. For example, it has been shown that for a different subfamily of metabelian groups the conjugacy search problem reduces to the DLP.

In August 2015 the National Security Agency (NSA) announced plans to upgrade security standards; the goal is to replace all deployed cryptographic protocols with quantum secure protocols. This transition requires a new security standard to be accepted by the National Institute of Standards and Technology (NIST).

One goal of cryptography, as it relates to complexity theory, is to analyze the complexity assumptions used as the basis for various cryptographic protocols and schemes. A central question is determining how to generate intractible instances of these problems upon which to implement an actual cryptographic scheme. The candidates for these instances must be platforms in which the hardness assumption is still reasonable. Determining if the group-based cryptographic schemes are quantum-safe begins with determining the groups in which these hardness assumptions are invalid in the quantum setting.

In what follows we address the quantum complexity of the Hidden Subgroup Problem (HSP) to determine the groups in which the hardness assumption still stands. The Hidden Subgroup Problem (HSP) asks the following: given a description of a group G and a function f from G to X for some finite set X is guaranteed to be strictly H-periodic, i.e. constant and distinct on left (resp. right) cosets of a subgroup $H < G$, find a generating set for H.

Group-based cryptography could be shown to be post-quantum if the underlying security problem is NP-complete or unsolvable; firstly, we need to analyze the problem's equivalence to HSP, then analyze the applicability of Grover's search problem.

Delaram Kahrobaei is a Professor and Chair of Cyber Security in the Department of Computer Science at the University of York as well as adjunct Professor at the New York University. Her recent interests are data mining over encrypted data, as well as post-quantum cryptography. Her research has been supported by grants from ONR, NSF, NSA, AAAS, NASA, IHP, AWM, RF-CUNY among others.