BOOK OF ABSTRACTS

Ryan Amiri (Heriot-Watt University)

Title: **Quantum Digital Signatures**

Abstract: Quantum digital signatures (QDS) allow a sender (Alice) to sign a message such that the receiver (Bob) can both verify that the message originated from Alice, has not been tampered with, and that a third party (Charlie) will agree that the message indeed came from Alice. With the development of quantum cryptography, QDS protocols have emerged that provide the above functionality with security based on the laws of quantum mechanics. The presentation gives an introduction to a simple QDS protocol, as well as some outlining some of the ideas and problems in the proofs of security.

Sarah Croke (University of Glasgow)

Title: **A quantum adaptive algorithm**

Abstract: Adaptive algorithms can update the rules for processing input data based on what has been read so far. An example is adaptive coding, in which the length of codeword assigned to a particular symbol depends on the current estimate of the probability with which that symbol occurs. Quantum adaptive algorithms are potentially problematic, since any attempt to learn about data results in disturbance. How can we learn about quantum data as it is read, without disturbing that data? I will talk about one example of a quantum adaptive algorithm, for the task of entanglement concentration. By extracting quantum information about data read so far, we can produce an adaptive, or streaming algorithm, which dramatically reduces the space requirements needed for this task.

Ross Duncan (University of Strathclyde)

Title: **Causality and Determinism in MBQC**

Abstract: The 1-way model is a quantum computer that works by performing single-qubit measurements on a large entangled state, the graph state. In order to perform deterministic computations the later measurements must depend on earlier measurements, and the dependence depends on the geometry of the state. I'll present a more abstract view of this model, formalised in ZX-calculus, and examine how causality and determinism interact.

Alexandru Gheorghiu (University of Edinburgh)

Title: **Entangled Servers vs. Single Server Quantum Verification**

Abstract: Quantum computing and quantum technologies have been developing rapidly in recent years. The benefits they can bring are numerous and well known. However, as far as we can tell, classical computations cannot scale up to the computational power of quantum mechanics, so then how can we verify the result of a computation mediated by quantum mechanics? This is what quantum verification aims to answer. In this presentation, I review and compare two existing protocols for performing quantum verification and show how they can be combined into an improved protocol that inherits advantages from both.

Theodoros Kapourniotis (University of Edinburgh

Title: **Quantum authentication and verification**

Abstract: While the success of quantum cryptography comes from improving the security of tasks involving classical messages, the security of quantum messages is also important. We present some basic elements of standard cryptographic tasks such as encrypting and authenticating quantum information over an untrusted channel, verifying the correctness of a quantum computation on an untrusted server and finally describe some connections between them.

Aleks Kissinger (University of Oxford)

Title: **Seeing Double**

Abstract: I will discuss a unique way to express and work with quantum channels, via the “doubling construction”. This approach, stemming from Selinger’s categorical “CPM-construction”, is now used as the basis of a master-level course in quantum information as well as a forthcoming textbook “Picturing Quantum Processes”. I will demonstrate how in this language notions such as causality, purification and non-signalling arise naturally, and give some indication of how it generalizes to the construction of quantum-like models, like Boolean-valued quantum theory.