THE FIELDS INSTITUTE
FOR RESEARCH IN MATHEMATICAL SCIENCES

ABSTRACTS 1.2

ANDRIS AMBAINIS
University of Waterloo

Multiparty quantum coin flipping

We consider information-theoretically secure quantum protocols for coin flipping. In the two-party case, there is a protocol in which no cheating party can fix the result to one value with probability more than 3/4. In contrast, in any classical protocol, one party can successfully cheat with probability 1.

We study the multiparty case when there are k parties and up to k-1 of them may be dishonest. We show that, even in this case, dishonest parties do not have a complete control over the outcome of the protocol. That is, we construct a protocol in which k-1 cheating parties can succesfully fix the outcome of the protocol with probability at most $1 - \Omega(1/k)$. We also show that this is optimal.

In our analysis, we introduce a new problem: two party coin flipping with a penalty for cheating. We design a protocol for this problem which we then use to design the multiparty protocol. We expect that this approach may be useful elsewhere.

We also discuss the possibility of quantum protocols for oblivious transfer in which no party can successfully cheat with probability 1.

Parts of this talk are joint work with Harry Buhrman, Yevgeniy Dodis, Hein Rohrig and Ran Canetti.

MICHAEL BEN-OR
Hebrew University of Jerusalem

Honest Private Computation with a Quantum Channel

HARRY BUHRMAN
CWI, Amsterdam

On the (Im)Possibility of Quantum String Commitment

Quantum bit commitment is impossible, but how far can we stretch the quantum limits when the task is to commit a string of n bits rather than a single bit?

"Not very far" is the answer that we obtain a from a no-go argument, where we invoke the Holevo information as the security criterion. In particular, our result implies the optimality of the trivial scheme, in which Alice sends a subset of b bits to Bob (commit phase) and later reveals the remaining n-b bits.

Things change dramatically, however, if we are willing to revise our standard of security and use the accessible information instead of the Holevo information. Based on the phenomenon of "locking" classical information into quantum states, we are able to design protocols which impose strong limitations on the ability of both parties to cheat.

This is joint work with Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo and Stephanie Wehner.

DANIEL GOTTESMAN
Perimeter Institute, Waterloo

Secure multiparty quantum computation

Suppose we have n players who wish to jointly perform a quantum computation, but some of their number are untrustworthy and are trying to learn privileged information and/or sabotage the computation. How many cheaters can we tolerate and still have a secure protocol? Secure multiparty classical computation is possible with fewer than n/3 cheaters, or fewer than n/2 when a secure broadcast channel is available. It turns out the same bounds hold in the quantum case. I will sketch the construction, which owes a great deal to the classical solutions, but requires a number of new components as well. This talk describes joint work with Ben-Or, Crepeau, Hassidim, and Smith.

SEAN HALLGREN
NEC, Princeton

Quantum algorithms and cryptography

An important goal in quantum computing is to determine which classical cryptosystems are secure in the presence of quantum computers. Shor showed that quantum computers can efficiently factor, and compute discrete logs over finite fields or elliptic curves, implying that quantum computers can break RSA and Diffie-Hellman. I will discuss this and its extension to number fields, resulting in quantum algorithms that can break the Buchmann-Williams key exchange protocol. I will also discuss which cryptosystems are currently secure against quantum computers.

PATRICK HAYDEN
McGill University, Montreal

The power of forgetting

Thermodynamics places surprisingly few fundamental constraints on information processing. In fact, most people would argue that it imposes only one, known as Landauer's Principle: a process erasing one bit of information must release an amount kT ln 2 of heat. It is this simple observation that finally led to the exorcism of Maxwell's Demon from statistical mechanics, more than a century after he first appeared. Ignoring the lesson implicit in this early advance, however, quantum information theorists have been relatively slow to embrace erasure as a fundamental primitive. Over the past year, however, it has become clear that a detailed understanding of how difficult it is to erase correlations

leads to a nearly complete synthesis and simplification of the known results of asymptotic quantum information theory. As it turns out, a great many tasks of interest, from distilling high-quality entanglement to sending quantum data through a noisy medium to many receivers, can be understood as variants of erasure. I'll sketch the main ideas behind these discoveries, including recent applications to network quantum communication, and end with some speculations on what lessons the new picture might have for understanding information loss in real physical systems.

DEBBIE LEUNG
IQC, Waterloo

QKD based on twisted ebits

We will present a scheme for QKD based on twisted ebits and prove its security. A consequence is that QKD can be security over a quantum channel with zero quantum capacity.

HOI-KWONG LO
University of Toronto

Decoy State Quantum Key Distribution: Theory and Practice

Decoy state quantum key distribution (QKD) has been proposed as a novel approach to improve dramatically both the security and the performance of practical QKD set-ups. We report the theory of the subject. Moreover, we report the world's first experimental demonstrations of decoy state QKD over 15km and 60km of commercial Telecom fibers, done by our group at the University of Toronto. Decoy state QKD is ready for immediate commercial applications.

NORBERT LUETKENHAUS
IQC, Waterloo

Challenges and directions in quantum key distribution

Quantum key distribution uses a quantum channel and an authenticated classical channel to distribute information theoretic secure key to two parties. The technical challenge is to build point-to-point connections that allow a high secure bit rate over lossy channels. I will briefly review the theoretical concepts of current schemes and their respective challenges. It is worth to note that some improvements can be done by improving the classical communication protocols that post-process the data. We show limitations for this situation. Finally, networks with some partial trust assumptions about repeaters can increase the usefulness of QKD applications.

DOMINIC MAYERS
Princeton University

Self-Testing of Quantum Circuits

We prove that a quantum circuit together with measurement apparatuses and EPR sources can be fully verified without any reference to some other trusted set of quantum devices. Our main assumption is that the physical system we are working with consists of several identifiable sub-systems, on which we can apply some given gates locally.

To achieve our goal we define the notions of simulation and equivalence. The concept of simulation refers to producing the correct probabilities when measuring physical systems. To enable the efficient testing of the composition of quantum operations, we introduce the notion of equivalence. Unlike simulation, which refers to measured quantities (i.e., probabilities of outcomes), equivalence relates mathematical objects like states, subspaces or gates.

Using these two concepts, we prove that if a system satisfies some simulation conditions, then it is equivalent to the one it is supposed to implement. In addition, with our formalism, we can show that these statements are robust, and the degree of robustness can be made explicit (unlike the robustness results of [DMMS00]). In particular, we also prove the robustness of the EPR Test [MY98]. Finally, we design a test for any quantum circuit whose complexity is linear in the number of gates and qubits, and polynomial in the required precision.

Joint work with Frederic Magniez, Michele Mosca and Harold Ollivier

ASHWIN NAYAK
University of Waterloo

Optimality of Approximate Encryption Schemes

Randomization of quantum states is the quantum analogue of the classical one-time pad. In earlier work, we noted an improved, efficient construction of an approximately randomizing map that uses $O(d/epsilon^2)$ Pauli operators to map any d-dimensional state to a state that is within epsilon (in trace distance) of the completely mixed state. This bound is a log d factor smaller than that of Hayden, Leung, Shor, and Winter (2004), and Ambainis and Smith (2004). In this talk, we will discuss the optimality of the above scheme via its connection to a new notion of pseudorandomness.

KENNY PATERSON
Royal Holloway, Egham

What can Quantum Cryptographers learn from History?

In this talk, I will discuss some of the pitfalls that "classical" cryptographers have fallen into over the years, with a view to helping quantum cryptographers avoid making similar mistakes in future. Examples will include: security proofs that have turned out to be wrong, security models that are incomplete, and implementations that are inadequate or do not follow recommendations from theory. I will attempt to explain the relevance of each example for quantum cryptography.

ALEXANDRE PAUCHARD
IDQuantique, Geneva

Integration of a commercial quantum cryptography appliance into metropolitan area networks

This talk will present id Quantiques implementation of a QKD system based on faint laser pulses. Perspectives on the challenges facing the deployment of practical QKD systems into existing network infrastructure will be covered in more details. Field testing experiments obtained in MAN networks will be presented.

ODED REGEV
Tel-Aviv University

On Lattices, Random Linear Codes, and Cryptography

I will describe some recent progress on lattice-based cryptosystems, focusing on a recent public-key cryptosystem presented in STOC 2005.

The security of this cryptosystem is based on the worst-case *quantum* hardness of SVP and SIVP. Previous lattice-based public-key cryptosystems such as the one by Ajtai and Dwork are based on unique-SVP, a special case of SVP. The new cryptosystem is much more efficient than previous cryptosystems: the public key is of size $\tilde{O}(n)$ and encrypting a message increases its size by $\tilde{O}(n)$ (in previous cryptosystems these values are $\tilde{O}(n^4)$ and $\tilde{O}(n^2)$, respectively).

RENATO RENNER
DAMTP, Cambridge

How secure is quantum key distribution?

A basic requirement for a cryptographic key distribution protocol (of any kind, classical or quantum) is that the generated key can be used as if it was a perfect key, i.e., a uniform random value unknown to any adversary. As reported recently (quant-ph/0512021), for quantum key distribution (QKD), this property is not implied by most of the established security definitions and security proofs. In particular, one-time pad encryption might be insecure if one uses a key generated by a QKD protocol. In the talk, we discuss possible solutions to this problem.

LOUIS SALVAIL
LRI, Orsay

A Tight High-Order Entropic Uncertainty Relation with Applications in the Bounded Quantum-Storage Model

We introduce a new entropic quantum uncertainty relation involving min-entropy. The relation is tight and customized for its use in quantum cryptography. We propose new strong security definitions for quantum 1-out-of-2 oblivious transfer (OT) and quantum bit commitment (BC) and provide a technique for proving security against dishonest receivers/committers. The uncertainty relation is used to prove security in this strong sense of protocols for OT and BC in the bounded quantum-storage model.

Joint work with Ivan Damgaard, Serge Fehr, Christian Schaffner, and Renato Renner.

BARRY SANDERS
University of Calgary

Real-World Quantum Cryptography in Calgary

A partnership between the University of Calgary (led by Wolfgang Tittel), the Southern Alberta Institute of Technology, and General Dynamics Canada, with support from NSERC and iCORE, is working to develop fast, secure quantum key distribution between points in Calgary. I will discuss practical obstacles and our plans to circumvent these problems by employing integrated electronics, fast detectors, and point-to-point protocols.

MIKLOS SANTHA
LRI, Orsay

An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups

Extraspecial groups, a subclass of p-groups, play an important role in the theory of this group family. They are also present in quantum information theory, in particular in quantum error correction, and in quantum computing in the context of the paradigmatic hidden subgroup problem. We give here an efficient algorithm for this problem in any extraspecial group. Our approach is quite different from the recent algorithms presented for the Heisenberg group, the extraspecial p- group of size p^3 and exponent p. Exploiting the automorphism structure of the groups we define specific group actions which are used to reduce the problem to hidden subgroup instances in abelian groups that can be dealt with directly. This is joint work with Gbor Ivanyos and Luc Sanselme

ADAM SMITH
Weizmann Institute, Rehovot

Techniques for Secure Distributed Computing with Quantum Data

We will begin by delving into some details of the techniques used for constructing protocols for secure distributed computation of arbitrary quantum circuits in networks with a majority of honest participants (this will follow up, at least partly, on the earlier talk by Daniel Gottesman). Time permitting, we will turn to two-party computing tasks and the connections between classical zero-knowledge and secure processing of quantum data.

ALAIN TAPP
IRO, Montreal

Private Quantum Channels

I will investigate how a classical private key can be used by two players, connected by an insecure one-way quantum channel, to perform private communication of quantum information. In particular we show that in order to transmit n qubits privately, 2n bits of shared private key are necessary and sufficient. This result may be viewed as the quantum analogue of the classical one-time pad encryption scheme. From the point of view of the eavesdropper, this encryption process can be seen as a randomization of the original state. We thus also obtain strict bounds on the amount of entropy necessary for randomizing n qubits.

THE FIELDS INSTITUTE
FOR RESEARCH IN MATHEMATICAL SCIENCES

ABSTRACTS 1.2

JOHN WATROUS
IQC, Waterloo

Quantum computational indistinguishability and zero-knowledge

In this talk I will discuss the notion of computational zero-knowledge in the quantum setting, and the related notion of quantum computational indistinguishability. An investigation of these notions reveals some interesting properties that are unique to quantum information, and suggest that particularly strict notions of security of quantum cryptographic primitives may be required in common settings. For example, a strong definition of indistinguishability for computationally concealing commitment schemes is (evidently) required for known quantum zero-knowledge proofs for NP.

GREGOR WEIHS
IQC, Waterloo

Experimental Quantum Key Distribution: Status and Directions

I will review the progress in experimental implementations, highlight the various firsts and finally present the status quo. I will talk about our own effort in entangled free-space quantum key distribution and discuss the various obstacles in achieving practical security and high key creation rates.