CRYPTASC Workshop

Program

Tuesday, October 6, 2009

- 9.00 am
On the Impossibility of Gaussian Bit Commitment
Loïck Magnin (Université Libre de Bruxelles)

Abstract:
Unconditionally secure bit commitment is forbidden by quantum mechanics. We extend this no-go theorem to continuous-variable protocols where both players are restricted to use Gaussian states and operations, which is a realistic assumption in current- state optical implementations.

- 9.40 am
Continuous-Variable Quantum Bit Commitment
Xavier Lacour (Université Libre de Bruxelles / Cryptasc)

Abstract:
Quantum bit commitment has been shown to turn into an interesting possible primitive if one puts some bound on the quantum memory that is available to both players. We investigate whether the same kind of approach can be applied to an optical continuous-variable scenario where the initial state is non-Gaussian but the cheating strategies are limited to Gaussian operations (i.e., beam splitters, phase shifters, and squeezers).

- 10.20 am
About Random Series obtained from a Quantum Random NumberGenerator (QRNG).
Thomas Durt and Frederik Vanden Berghe (Vrije Universiteit Brussel / Cryptasc)
Abstract:
Our colleagues from the ULB have developed a QRNG based on vacuum fluctuations. We have analyzed the randomness properties exhibited by the bit series generated by their QRNG and found some correlations that can be shown to result from the continuity or inertia of the stochastically fluctuating signal that is used in order to generate the bits. The deep understanding of these departures from "perfect" randomness also opens the way for "randomness increasing" methods that we successfully implemented. These techniques could be applied to the diagnosis and therapy of any RNG based on physical fluctuations of a continuous signal.

- 11.00 am
Coffee Break

- 11.30 am

Secret Keys and Random Numbers From Quantum Non-Locality.
Serge Massar (Université Libre de Bruxelles / Cryptasc)

Abstract:
Non local correlations are obtained when local measurements are carried out on entangled quantum particles, leading to a violation of a Bell inequality. We discuss how such non local correlations shared can be used to generate random numbers and secret keys. Using non locality allows a higher degree of security than in the more traditional approaches to quantum cryptography, as it is no longer necessary to trust ones devices, nor even to trust quantum mechanics. We will briefly present the first experimental realization of these proposals, carried out at NIST by the group of C. Monroe.

- 12.10 pm

Entanglement Equivalence of Symmetric N-qubit states
Thierry Bastin (Université de Liège)

Abstract:
We study the interconversion of multipartite symmetric N-qubit states under stochastic local operations and classical communication (SLOCC). We demonstrate that if two symmetric states can be connected with a non-symmetric invertible local operation (ILO), then they belong necessarily to the separable, W, or GHZ entanglement class, establishing a practical method of discriminating subsets of entanglement classes. Furthermore, we prove that there always exists a symmetric ILO connecting any pair of symmetric N-qubit states equivalent under SLOCC, simplifying the requirements for experimental implementations of local interconversion of those states.

- 12.50 pm
Lunch break

- 14.30 pm

Interacting Quantum Observables: Categorical Algebra and Diagrammatics
Ross Duncan (University of Oxford)
Abstract:

Within an intuitive diagrammatic calculus and corresponding high-level category-theoretic algebraic description we axiomatise complementary observables for quantum systems described infinite dimensional Hilbert spaces, and study their interaction. We also axiomatise the phase shifts relative to an observable. The resulting graphical language is expressive enough to denote any quantum physical state of an arbitrary number of qubits, and any processes thereof. The rules for manipulating these result in very concise and straightforward computations with elementary quantum gates, translations between distinct quantum computational models, and simulations of quantum algorithms such as the quantum Fourier transform. They enable the description of the interaction between classical and quantum data in quantum informatic protocols. More specifically, we rely on the previously established fact that in the symmetric monoidal category of Hilbert spaces and linear maps non-degenerate observables correspond to special commutative y-Frobenius algebras. This leads to a generalisation of the notion of observable that extends to arbitrary y-symmetric monoidal categories (†-SMC). We show that any observable in a †-SMC comes with an abelian group of phases. We define complementarity of observables in arbitrary †-SMCs and

prove an elegant diagrammatic characterization thereof. We show that an important class of complementary observables give rise to a Hopf-algebraic structure, and provide equivalent characterisations thereof.

- 15.10 pm

Calculating with the square root of NOT
Alexis De Vos (University of Gent)

Abstract:
Classical reversible computing with n bits forms a group isomorphic to the finite symmetric group S2n. Quantum computing with n qubits forms a group isomorphic to unitary Lie group U(2n). We add to the classical reversible logic gates, two extra gates, i.e. the square root of NOT and the controlled square root of NOT. This leads to a new kind of calculus, situated between classical reversible computing and quantum computing. It is isomorphic to a discrete group with a (countably) infinite order.

- 15.50 pm

A Measurement-based Quantum Virtual Machine
Yves Vandriessche (Vrije Universiteit Brussel / Cryptasc)

Abstract:
In this talk we present a virtual machine for quantum computations. A virtual machine is a common abstraction technique in computer science which provides a platform to deal with variation in both high- level languages and low-level computation machine models. The Quantum Virtual Machine (QVM) toolset we present consists of a specification, assembler and evaluator tool. The specification tool provides a graphical user interface which allows easy definition and combination of measurement patterns in a way akin to drawing quantum circuits. The assembler translates these specifications into code that can be understood by the evaluator. The latter executes a small instruction set based on the measurement calculus, a model which unites both, compactness and universality. Our QVM has the additional benefit of unifying both the execution model and the semantic model used by existing formal verification techniques for quantum programs. This will prove useful in our future application of the QVM to the security analysis of quantum cryptographic protocols.

- 16.30pm

Coffee break

- 16.45pm

What is a use case for quantum key exchange?
Daniel J. Bernstein (University of Illinois at Chicago)
Tanja Lange (Technische Universiteit Eindhoven)

Abstract:
From Paterson, Piper, and Schack's "Why quantum cryptography?" to Stebila, Mosca, and Lutkenhaus' "The Case for Quantum Key Distribution" the search for a killer application of quantum key exchange has been a topic of intense discussion. In our contribution we will explain the effect quantum computers have on conventional cryptography and the consequences for the choice of algorithms and keysizes. We will also explain how to narrow the search space for applications where quantum cryptography could be better than conventional cryptography.

- 17.25pm

Remarks on quantum secret sharing & the complexity of Shor's algorithm for factorization
Cao Zhengjun (Université Libre de Bruxelles / Cryptasc)

Abstract

(1) Key establishment is a process whereby a shared secret becomes available to two or more parties. The idea of secret sharing is to start with a secret, and divide it into pieces called shares which are distributed amongst users in such a way that the pooled shares of specific subsets of users allow reconstruction of the original secret. In this presentation, we remark that many quantum secret sharing schemes are not secret sharing schemes but rather key establishment schemes. Actually, these key establishment models are somewhat different from BB84.

(2) Shor's algorithm for factorization uses two quantum registers. An observer has to measure the final quantum state in the first register and interpret the measurement result as a scalar. In this presentation, we show that the complexity of the algorithm should be expressed by a conditional probability rather than a joint probability.

- 18.05pm
Closing

Venue

The workshop will take place at the Université Libre de Bruxelles in auditorium UA3.219, on the 1st floor (level 3) in building U, entrance door A, in the campus Solbosch (Ixelles). After entering building U from entrance A, climb the stairs on your left then turn left again and climb a few more steps to get to level 3. Then, look for the door UA3.217, with the sign

Center for Quantuim Information and Communication (QuIC).