09311 Abstracts Collection
Classical and Quantum Information Assurance Foundations and Practice
— Dagstuhl Seminar —

Samuel L. Braunstein[1], Hoi-Kwong Lo[2], Kenny Paterson[3] and Peter Y. A. Ryan[4]

[1] University of York, GB
schmuel@cs.york.ac.uk
[2] University of Toronto, CDN
hklo@comm.utoronto.ca
[3] Royal Holloway Univ. - London, GB
kenny.paterson@rhul.ac.uk
[4] University of Luxembourg, LU
peter.ryan@uni.lu

Abstract. From 26 July 2009 to 31 July 2009, the Dagstuhl Seminar 09311 "Classical and Quantum Information Assurance Foundations and Practice" was held in Schloss Dagstuhl – Leibniz Center for Informatics. The workshop was intended to explore the latest developments and discuss the open issues in the theory and practice of classical and quantum information assurance. A further goal of the workshop was to bring together practitioners from both the classical and the quantum information assurance communities. To date, with a few exceptions, these two communities seem to have existed largely separately and in a state of mutual ignorance. It is clear however that there is great potential for synergy and cross-fertilization between and this we sought to stimulate and facilitate.

The program included tutorials from both communities aimed at bringing members of the the other camp up to speed:

- Intro to modern cryptography (Bart Preneel)
- Intro to provable security (Kenny Paterson)
- Intro to the modelling and formal analysis of cryptographic protocols (Peter Ryan)
- Intro to the theory of quantum cryptography (Charles Bennett)
- Towards quantum key distribution with testable assumptions: a tutorial (Hoi-Kwong Lo)
- Introduction to Universal Composability (Dominique Unruh)
- Practical aspects of QKD (Gregoire Ribordy)

The workshop generated simulating and at times heated debates on the merits and demerits of quantum cryptography. A participant from the conventional cryptography community claimed that quantum cryptography is essentially useless in practice because of its high cost, low key rate, short distance, limited applications and the need to distribute the

Dagstuhl Seminar Proceedings 09311
Classical and Quantum Information Assurance Foundations and Practice
http://drops.dagstuhl.de/opus/volltexte/2010/2365

initial authentication key material. Moreover, his view was that quantum cryptography is not an effective counter-measure against the threat of quantum computing. He believed that public key cryptographic systems such as NTRU and McEliece could be used, if a quantum computer were ever built in future.

The quantum community countered as follows. First, there is a need for top secret long-term security and quantum cryptography can never reduce security. Second, to break a quantum cryptographic system, one needs to eavesdrop today because there is no classical transcript for a quantum communication. This means an eavesdropper has to invest in quantum technologies in order to eavesdrop. Third, current technological limitations of quantum cryptography such as key rate and distance may be overcome in future. For instance, quantum repeaters could, in principle, extend the distance of quantum cryptography arbitrarily. Fourth, the cost of the quantum cryptographic systems may be absorbed through savings in multiplexing of optical channel in telecom fibers. Fifth, since few quantum people are working on breaking NTRU or McEliece cryptosystems these days, the security of those systems against quantum attacks is largely unknown.

Perhaps, a more balanced view to take is that it is important to explore future cryptographic infra-structure. Quantum cryptography, while probably not the only solution, may well play a part in such a future infra-structure.

During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. Links to extended abstracts or full papers are provided, where available.

Keywords. Quantum Information assurance, classical information assurance, cryptography, quantum computation

Measuring Entanglement with Universal Time-Bin Qubit Analyzers

After an introduction into basic tools of quantum communication, qubits and entangled qubits, I will motivate the importance of entanglement for understanding nature at the quantum level as well as for applications in quantum cryptography and communication. I will then introduce how one can create and measure photons and pairs of photons (in product as well entangled states) in the laboratory, and discuss a new experiment that demonstrates the first measurement of time-bin entangled qubits using universal time-bin qubit analyzers. Our measurement, which relies on the conversion of time-bin qubits into polarization qubits followed by polarization measurements, yields violations of the CHSH-Bell inequality and paves the road for tests of the Leggett inequality with time-bin qubits. Furthermore, as explained in the presentation by G. Brassard, our source has already been used for quantum coin flipping, and is promising

for hybrid quantum networks consisting of free-space and fibre-optics links and requiring encoding of quantum information in polarization as well as time-bin qubits.

Keywords: Quantum Communication, Entanglement

Joint work of: Bussières, Felix; Slater, Joshua; Jin, Jeongwan; Godbout, Nicolas; Tittel, Wolfgang

Is quantum information useful for security?

Romain Alleaume (ENS Telecommunications - Paris, FR)

I will try to partially answer, based on a review on recent work, the following question:

Can QKD and more generally quantum information be useful to cover some practical security requirements in current (and future) IT infrastructures?

I will in particular cover the following topics

- practical performances of QKD
- QKD network deployment - SECOQC project
- Capabilities of QKD as a cryptographic primitive - comparative advantage with other solution, in order to cover practical security requirements

Keywords: QKD, QKD networks

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2361

See also: http://arxiv.org/abs/quant-ph/0701168

Quantum Cryptography Tutorial

Charles H. Bennett (IBM TJ Watson Research Center, US)

After surveying the basics of quantum information (superposition, quantum gates and measurements, the no-cloning theorem, entanglement, and the meaning of the density matrix), I review the impact of quantum information on the goals of cryptography and information security, including the theory and practice of quantum key distribution, the no-go theorem for bit commitment, quantum secret sharing and distributed computation, and quantum cryptanalysis.

Keywords: Quantum information entanglement QKD cryptography cryptanalysis

Publicity, Privacy and forgetfulness in Nature

Charles H. Bennett (IBM TJ Watson Research Center, US)

The most private information, exemplified by which path a particle takes through an interferometer, is quantum: after the experiment is over even God doesn't remember what "happened". Less private are classical secrets, facts known only to a few, or information like the lost literature of antiquity that once was public but has been forgotten over time. Finally there is information that has been replicated and propagated so widely as to be infeasible to conceal and unlikely to be forgotten. Modern information technology has caused an explosion of such information, with the beneficial side effect of making it harder for tyrants to rewrite the history of their misdeeds; and it is tempting to hope that all macroscopic information is permanent, making such cover-ups impossible in principle. However, by comparing entropy flows into and out of the Earth with estimates of the planet's storage capacity, we conclude that most macroscopic information for example the pattern of drops in last week's rain shower or rice grains in last night's dinner is impermanent, eventually becoming nearly as ill defined, from a terrestrial perspective, as the which-path information of an interferometer.

Keywords: Quantum information privacy forgetfulness permanence

How to improve the price-performance ratio of quantum collision search

Daniel Bernstein (University of Illinois - Chicago, US)

A quantum algorithm by Brassard, Hoyer, and Tapp finds collisions in a generic b-bit hash function using $O(2^{b/3})$ calls to the hash function. How well does the same algorithm perform in more sophisticated cost measures than number of hash calls? In particular, does the algorithm achieve an optimal tradeoff between the size of a quantum computer and the time taken by the computer to find collisions? This talk will show that the algorithm is highly suboptimal from this perspective, and will explain how to do better.

Cost-benefit analysis of quantum cryptography

Daniel Bernstein (University of Illinois - Chicago, US)

"Why quantum cryptography?" "SECOQC white paper on quantum key distribution and cryptography." "Quantum cryptography: as awesome as it is pointless." "The case for quantum key distribution."

Different authors have come to wildly different conclusions regarding the value of quantum cryptography. Some of this variability can be explained by

implicit differences in models of what users value; this talk will present a unified analysis explicitly parametrized by the model. A surprisingly large part of the variability stems from easily correctable errors; this talk will explain how future authors can recognize and avoid the most common pitfalls.

Loss-Tolerant Quantum Coin Flipping

Gilles Brassard (Université de Montréal, CA)

Coin flipping is a cryptographic primitive in which two spatially separated players, who do not trust each other, wish to establish a common random bit. If we limit ourselves to classical communication, this task requires either assumptions on the computational power of the players or it requires them to send messages to each other with sufficient simultaneity to force their complete independence. Without such assumptions, all classical protocols are so that one dishonest player has complete control over the outcome. If we use quantum communication, on the other hand, protocols have been introduced that limit the maximal bias that dishonest players can produce. However, those protocols would be very difficult to implement in practice because they are susceptible to realistic losses on the quantum channel between the players or in their quantum memory and measurement apparatus. In this talk, we introduce a novel quantum protocol and we prove that it is completely impervious to loss. The protocol is fair in the sense that either player has the same probability of success in cheating attempts at biasing the outcome of the coin flip. We also give explicit and optimal cheating strategies for both players. Furthermore, we report on our successful implementation of the protocol.

Keywords: Coin flipping, loss tolerance, unconditional security, experiments

Joint work of: Berlin, Guido; Brassard, Gilles; Bussieres, Felix; Godbout, Nicolas; Slater, Joshua A.; Tittel, Wolfgang

Full Paper:
http://arxiv.org/abs/0904.3945

Full Paper:
http://arxiv.org/abs/0904.3946

See also: to appear in Physical Review A

Post-quantum cryptography

Tanja Lange (TU Eindhoven, NL)

Overview talk of the possibilities of post-quantum cryptography, that is cryptography that are conjecturally secure against attacks by quantum computers (and, of course, secure against attacks with classical computers).

Such crypto primitives include Merke hash trees and multivariate cryptography for signatures and lattice and code based crypto for encryption.

Together with Bernstein and Peters we have some recent results on attacking code-based cryptography.

Keywords: Post-quantum cryptography, Merkle hash trees, lattice-based, McEliece, code-based, multivariate

Full Paper:
http://www.pqcrypto.org

Towards QKD with testable assumptions

Hoi-Kwong Lo (University of Toronto, CA)

There is a big gap between the theory and practice of quantum key distribution (QKD). In principle, QKD offers unconditional security guaranteed by the laws of physics. In practice, all security proofs are based on specific physical models of a QKD system. A physical model contains assumptions. When an assumption of a physical model is violated, a security proof for a QKD system falls apart. In this talk, I will review standard assumptions in security proofs (including the single mode assumption and phase randomization assumption) and discuss how they might be enforced in practice. Moreover, I will discuss our recent work on proving the security of QKD with an untrusted source. Furthermore, I will describe our recent quantum hacking experiment against a commercial QKD system. Here, I exploit the detection efficiency mismatch between two detectors. In particular, I show how an eavesdropper, Eve, can violate the fair sampling assumption (in Bell-inequality testing or in QKD) by manipulating an ancillary variable (e.g. arrival time of a quantum signal). I will conclude by pointing out some future directions.

Keywords: Quantum cryptography

Geometry of abstraction in quantum computation

Dusko Pavlovic (University of Oxford, GB)

Modern cryptography is based on various assumptions about computational hardness and feasibility. But while computability is a very robust notion (cf Church's Thesis), feasibility seems quite sensitive to the available computational resources. A prime example are, of course, quantum channels, which provide feasible solutions of some otherwise hard problems; but ants' pheromones, used as a computational resource, also provide feasible solutions of other hard problems. So at least in principle, modern cryptography is concerned with the power and availability of computational resources.

The standard models, used in cryptography and in quantum computation, leave a lot to be desired in this respect. They do, of course, support many interesting solutions of deep problems; but besides the fundamental computational structures, they also capture some low level features of particular implementations. In technical terms of program semantics, our standard models are not *fully abstract*. (Related objections can be traced back to von Neumann's "I don't believe in Hilbert spaces" letters from 1937.)

I shall report on some explorations towards extending the modeling tools of program semantics to develop a geometric language for quantum protocols and algorithms. Besides hiding the irrelevant implementation details, its abstract descriptions can also be used to explore simple nonstandard models. If the time permits, I shall describe a method to implement teleportation, as well as the hidden subgroup algorithms, using just abelian groups and relations.

Keywords: Quantum algorithms, categorical semantics, Frobenius algebra, classical structure

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2362

An Introduction to "Modern" Cryptology

Bart Preneel (K.U. Leuven, BE)

Our talk has presented an overview of the status of modern (classical) cryptology. We have compared the challenges in communications and computer security settings, historically known as COMSEC and COMPUSEC respectively. We have discussed the evolving attack models: first the communicating parties Alice and Bob want to protect themselves against an opponent, subsequently Alice or Bob can be malicious; today we also consider a setting in which Alice tries to subvert the cryptographic device provided by a third party (e.g. in the context of Digital Rights Management). In this setting implementation level attacks are important. In a second part of the talk we have given an overview of the state of the art and challenges for several cryptographic primitives: block ciphers, hash functions, MAC algorithms, public key encryption and digital signatures. We have concluded with a discussion on the relation between applications, protocols, primitives, building blocks, and cryptographic assumptions.

Keywords: Cryptology, models, implementation attacks, block ciphers, hash functions, MAC algorithms, public key encryption

Poled Fibre, with a Twist: Towards polarization-entangled photon pair generation in poled silica fiber

Li Qian (University of Toronto, CA)

Polarization entangled photon pairs are an important resource used in quantum cryptography.

They are typically generated via spontaneous parametric down conversion (SPDC) processes in a nonlinear optical crystal, and then collected into an optical fiber for long-distance transmission, such as in the case of quantum key distribution. Alternatively, entangled photon pairs can be generated directly in fiber, which is more appealing because it eliminates the bulky and lossy fiber coupling stage. High flux of entangled photon pairs can potentially be achieved in fiber, where the interaction length for the SPDC process can be made large. Additionally, unlike with nonlinear crystals, properties such as birefringence and dispersion can be easily tailored through fiber design.

However, SPDC processes cannot take place in conventional fiber because silica, being isotropic, lacks the required second-order nonlinearity. Current research on in-fiber generation of entangled photons has been concentrated on the spontaneous four-wave-mixing (SFWM) processes, which uses the third-order nonlinearity of silica glass. SFWM processes, while successful in producing entangled photon pairs, also have limitations, most notably, the contamination from Roman scattering.

We are investigating an alternative approach of generating entangled photon pairs - using thermally poled silica fiber, which exhibits an effective second-order nonlinearity ($\chi^{(2)}$). The advantages of this approach, as compared with the SFWM approach, include: (1) The required interaction length for efficient SPDC is much smaller; (2) Quasi-phase matching is possible through a periodic erasure of induced $\chi^{(2)}$ by UV exposure, giving much flexibility to the choice of pump, signal, and idler wavelengths; (3) Raman scattered photons are spectrally well separated from the signal and the idler, eliminating the need for cryogenic cooling; (4) Suppressing the pump photons at the output is made much easier due to the large wavelength separation between the pump and its daughter photons, and can be implemented with fibre-based filters; (5) Maximally polarization entangled photons can be directly generated in this $\chi^{(2)}$ fibre in a straightforward way. In this talk, I will present the factors that need to be considered in this approach, including:

- How to optimize the second-order nonlinearity during thermal poling
- How to achieve (quasi) phase matching for the SPDC process
- The consequence of fiber birefringence and how to determine the values of the individual $\chi^{(2)}$ tensor elements
- The consequence of fiber twisting and how to utilize it to enhance a specific SPDC process for generation of entangled photon pairs.

Keywords: Entangled photon generation, SPDC, nonlinear fiber, thermally poled fiber

Tutorial: Modelling and Analysis of Security Protocols

Peter Ryan (University of Luxemburg, LU)

A tutorial on concepts and technqiues in the design and analysis of classical cryptographic protocols.

Keywords: (Classical) cryptographic protocols, formal analysis technqiues and tools

Limited-Quantum-Storage Cryptography: From Theory to Practice

Christian Schaffner (CWI - Amsterdam, NL)

In 2005, the idea of basing the security of two-party quantum protocols on the difficulty of storing quantum information has been proposed. In this talk, I will give an overview over the developments in this research area.

I will cover the basic protocol for 1-2 oblivious transfer and touch on more recent issues such as composable security definitions and practical implementation problems the latter of which are similar to those encountered in quantum key distribution.

Keywords: Quantum cryptography, two-party protocols, limited quantum storage

Universally Composable Quantum Oblivious Transfer

Dominique Unruh (Universität des Saarlandes, DE)

We show that a statistically secure, universally composable quantum oblivious transfer protocol can be realized from a commitment functionality.

Hence it is possible to construct universally composable, statistically secure protocols for any reactive functionality from a commitment.

This stands in contrast to the classical setting where this is known to be impossible. Furthermore, we discuss connections to long-term security.

Keywords: Quantum cryptography, oblivious transfer, universal composability

Full Paper:
http://arxiv.org/abs/0910.2912v1

See also: Technical Report, arXiv:0910.2912v1 [quant-ph]