<table>
<thead>
<tr>
<th>Speaker's name and affiliation</th>
<th>Talk title</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotem Arnon-Friedman (ETH Zürich)</td>
<td>de Finetti reductions in the context of non-local games</td>
<td>Device independent (DI) protocols, such as randomness expansion and amplification, received huge attention in the last several years, and yet, no generally applicable method to exploit symmetry and simplify the analysis of complex DI tasks has been known. In a talk we would like to present a new de Finetti theorem, specialised for the device independent setting, with its first application to parallel repetition of non-local games.</td>
</tr>
<tr>
<td>Ulrik L. Andersen (Technical University of Denmark)</td>
<td>Continuous variable quantum key distribution</td>
<td>Continuous variable quantum key distribution (CVQKD) is based on the coherent detection of Gaussian states in phase space using homodyne detectors. In my talk I will discuss four different realizations of CVQKD: 1) Measurement device independent CVQKD 2) Squeezed light based CVQKD 3) CVQKD using noisy coherent states 4) Single quadrature CVQKD.</td>
</tr>
<tr>
<td>Cédric Bamps (Université Libre de Bruxelles)</td>
<td>Robust self-testing of partially entangled systems and its application to randomness expansion</td>
<td>In this talk, I will show that the tilted CHSH inequalities (Acín et al., 2012) are robust, strong self-tests for their maximally violating reference systems: in a black-box scenario where the expected violation of a tilted CHSH inequality achieves the quantum maximum up to a small error, the underlying quantum system is guaranteed to be the reference system, up to vanishing terms of optimal order in the violation error. Interestingly, this family of inequalities covers all partially entangled qubit states as reference systems. This raises the question of how much entanglement is needed for device-independent randomness expansion. I will talk about work in progress to exploit the self-testing property of the tilted CHSH inequalities to expand randomness from a given amount of entanglement diluted into many weakly entangled states.</td>
</tr>
<tr>
<td>Jean-Daniel Bancal (National University of Singapore)</td>
<td>Device-independent entanglement characterization and beyond</td>
<td>Entanglement characterization is a preliminary step in the implementation of many quantum information processing tasks. In this talk, I will describe some recent progress on the possibility to characterize entanglement in a device-independent manner, i.e., directly from the observed measurement statistics without relying on any assumption about the systems observed or of the measurements performed. In particular, I will describe a technique that allows for the characterization of correlations derived from quantum states having additional property, such as positive partial transposition. This, in turn, permits the quantification of entanglement as well as the certification of many-body entanglement (i.e., entanglement depth) in a device-independent manner. Specifically, from the observed correlations or the amount of violation of a given Bell inequality, we can provide non-trivial lower bounds on the amount of (genuine) negativity present in the measured quantum state and/or the extent to which it is many-body entangled. The bounds on negativity, in turn, provide further information about the dimension of the underlying Hilbert space and/or the type of entanglement responsible for the observed correlations.</td>
</tr>
<tr>
<td>Mario Berta (California Institute of Technology)</td>
<td>Semidefinite programming hierarchies for quantum adversaries</td>
<td>I will present work with Omar Fawzi and Volkher Scholz, where we give a unifying approach to understand the stability properties of randomness extractors against quantum adversaries. We propose a converging hierarchy of semidefinite programs that gives increasingly tight characterizations of quantum-proof extractors.</td>
</tr>
<tr>
<td>Kai-Min Chung (Academia Sinica)</td>
<td>Randomness Extractors: from Classical to Quantum Worlds</td>
<td>Randomness extractors are deterministic functions that extract an almost-uniform random source from weak sources of randomness. Extractors are quantum-proof if the extraction works even in presence of quantum side-information (of the sources). Since their invention, extractors have found wide-range of applications in theoretical computer science beyond their original motivation. In this talk, I will survey various notions of randomness extractors and their quantum-proof variant, with focus on the notion of (quantum-proof) seeded extractors. I will review some recent developments, highlight gaps of our understanding in the quantum setting, and discuss some</td>
</tr>
</tbody>
</table>
challenges towards bridging the gaps. I will also motivate further study on quantum-proof randomness extraction in some cryptographic settings.

| Matthew Coudron  
(Massachusetts Institute of Technology) | Interactive proofs with approximately commuting provers | I will present work with Thomas Vidick, in which we study a hierarchy of semidefinite programs, introduced independently by Pironio et al. and Doherty et al., for estimating the winning probability of non-local entangled games. In particular, we introduce a rounding scheme for the hierarchy, establishing that any solution to its $N$-th level can be mapped to a strategy for the game in which measurement operators associated with distinct players have pairwise commutator bounded by $O(\ell^2/\sqrt{N})$ in operator norm, where $\ell$ is the number of possible answers per player. I will discuss how, under a certain long standing mathematical conjecture, this implies a (doubly exponential) upper bound on MIP*. I will also discuss independent applications. |
| --- | --- | --- |
| Joseph Fitzsimons  
(Singapore University of Technology and Design) | Towards homomorphic encryption secured by the laws of physics | One of the major advances in modern cryptography has been the advent of fully homomorphic encryption. Homomorphic encryption allows data to be processed in an encrypted form without access to the key, and as such has a myriad of applications in secure computing. All known schemes which allow for universal computation on encrypted data, termed fully-homomorphic, derive their security from assumptions concerning the intractability of certain computational problems. In this talk, I will address the question of whether quantum mechanics allows for unconditionally secure fully-homomorphic encryption schemes. I will begin by presenting a negative result: no scheme which is both compact and fully-homomorphic can have accessible information exactly equal to zero. Surprisingly, however, this statement is not known to hold if the constraint on accessible information is relaxed to allow for non-zero leakage of information. I will discuss the construction of encryption schemes which allow non-classical processing of the encrypted data in which the accessible information is bounded. |
| Karol Horodecki  
(University of Gdańsk) | Randomness amplification with two devices | Recently the first physically realistic protocol amplifying the randomness of Santha-Vazirani sources using a finite number of no-signaling devices and with a constant rate of noise has been proposed, however there still remained the open question whether this can be accomplished under the minimal conditions necessary for the task. Namely, is it possible to achieve randomness amplification using only two no-signaling devices and in a situation where the violation of a Bell inequality implies only an upper bound for some outcome probability for some setting combination? Here, we solve this problem and present the first device-independent protocol for the task of randomness amplification of Santha-Vazirani sources using a device consisting of only two non-signaling components. We show that the protocol can amplify any such source that is not fully deterministic into a totally random source while tolerating a constant noise rate and prove the security of the protocol against general no-signaling adversaries. The minimum requirement for a device-independent Bell inequality based protocol for obtaining randomness against no-signaling attacks is that every no-signaling box that obtains the observed Bell violation has the conditional probability $P(x|u)$ of at least a single input-output pair $(u,x)$ bounded from above. We show how one can construct protocols for randomness amplification in this minimalistic scenario. |
| Hermann Kampermann  
(Heinrich Heine University Düsseldorf) | Graph state quantum repeater networks | We show how general graph states can be distributed over large distances via a quantum repeater network. This goal is achieved with a one-way repeater scheme and an error correction codes in the language of graph states. A general error analysis is presented accounting for imperfect preparation, imperfect quantum gates, losses and detection errors. The scheme is exemplified by the 7-qubit Steane code and the quantum Golay code. See http://arxiv.org/abs/1504.06599. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elham Kashefi (University of Edinburgh)</td>
<td>On optimising quantum communications in verifiable quantum computing</td>
<td>In the absence of any efficient classical schemes for verifying quantum computing, the importance of limiting the required quantum resources has been highlighted recently. Currently all existing verification methods are based on cryptography techniques where an almost classical verifier executes his desired encrypted quantum computation remotely on an untrusted quantum server. In this work we present a new efficient protocol for quantum verification by incorporating existing techniques in a non-standard composition to reduce the required quantum communications between the verifier and the server.</td>
</tr>
<tr>
<td>Stacey Jeffery (California Institute of Technology)</td>
<td>Quantum homomorphic encryption for circuits of low T-gate complexity</td>
<td>Fully homomorphic encryption is an encryption method with the property that any computation on the plaintext can be performed by a party having access to the ciphertext only. We give schemes for quantum homomorphic encryption, which is the encryption of quantum information such that quantum computations can be performed given the ciphertext only, in the setting of standard cryptographic security under computational assumptions (specifically, IND-CPA security), which we formally define for quantum information. Our schemes allow for arbitrary Clifford group gates, but become inefficient for circuits with large complexity, measured in terms of the non-Clifford portion of the circuit (we use the &quot;pi/8&quot; non-Clifford group gate, which is also known as the T-gate). Two schemes are proposed: the first scheme has a decryption procedure whose complexity scales with the square of the number of T-gates (compared with a trivial scheme in which the complexity scales with the total number of gates); the second scheme uses a quantum evaluation key of length given by a polynomial of degree exponential in the circuit's T-gate depth, yielding a homomorphic scheme for quantum circuits with constant T-depth. Both schemes build on a classical fully homomorphic encryption scheme. This talk is based on joint work with Anne Broadbent.</td>
</tr>
<tr>
<td>Charles Ci Wen Lim (University of Geneva)</td>
<td>Bridging the gap between the theory and practice of device-independent quantum information processing</td>
<td>I will present our latest work on self-testing QRNG and ideas to import DIQIP concepts into practical quantum cryptography.</td>
</tr>
<tr>
<td>Norbert Lütkenhaus (University of Waterloo)</td>
<td>Trusted and untrusted repeater for QKD</td>
<td>I will present our results on simplified trusted nodes, and also on quantum repeater technologies to beat the Takeoka-Guha-Wilde bound for long distance quantum communication.</td>
</tr>
<tr>
<td>Matthew McKague (University of Otago)</td>
<td>Interactive proofs for BQP via self-tested graph states</td>
<td>Using the measurement-based quantum computation model, we construct interactive proofs with non-communicating quantum provers and a classical verifier. Our construction gives interactive proofs for all languages in BQP with a polynomial number of quantum provers, each of which, in the honest case, performs only a single qubit measurement.</td>
</tr>
<tr>
<td>Speaker</td>
<td>Title</td>
<td>Abstract</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| Carl Miller  
*University of Michigan* | Randomness expansion in the presence of a quantum adversary | How can a classical user generate randomness from a quantum device that she does not trust? This problem was posed as early as 2006, but fully secure solutions have only appeared in the last few years. The current solutions are based on the idea that any device which violates a Bell inequality must be exhibiting quantum behavior, and therefore its outputs must be partially random. I will talk about recent results by Yaoyun Shi and myself on this problem, which include the first proof that any violation of the CHSH inequality can be used to generate fully secure random numbers. I will discuss how we overcame the central problem of proving security against an entangled quantum adversary, a problem which leads to some interesting mathematics. |
| Christopher Monroe  
*University of Maryland* | Quantum Networks with Atomic Nodes and Photonic Links | Trapped atomic ions are standards for quantum memory, and in addition to the ability to form local entangled networks with from their Coulomb interaction, trapped ion qubits can also be connected via photonic links over long distances. This modular architecture is well-suited for quantum networks for communications applications such as secure multiparty protocols and private random number generation. |
| Carlo Ottaviani  
*University of York* | High-rate measurement-device independent quantum key distribution | Quantum cryptography achieves a formidable task—the remote distribution of secret keys by exploiting the fundamental laws of physics. Quantum cryptography is now headed towards solving the practical problem of constructing scalable and secure quantum networks. A significant step in this direction has been the introduction of measurement-device independence, where the secret key between two parties is established by the measurement of an untrusted relay. Unfortunately, while qubit-implemented protocols can reach long distances, their key rates are typically very low, unsuitable for the demands of a metropolitan network. Here we show, theoretically and experimentally, that a solution can come from the use of continuous-variable systems. We design a coherent-state network protocol able to achieve remarkably high key rates at metropolitan distances, in fact three orders of magnitude higher than those currently achieved. Our protocol could be employed to build high-rate quantum networks where devices securely connect to nearby access points or proxy servers. |
| Rene Peralta  
*US National Institute of Standards and Technology* | The NIST Randomness Beacon and Applications | Tables of random numbers have been used for multiple purposes at least since the Industrial Revolution. In the digital age, algorithmic random number generators have largely replaced these tables. I will describe the NIST Randomness Beacon. This is an online resource that expands the use of randomness to multiple scenarios in which the latter methods cannot be used. The extra functionalities stem mainly from three features. First, the Beacon-generated numbers cannot be predicted before they are published. Second, the public, time-bound, and authenticated nature of the Beacon allows a user application to prove to anybody that it used truly random numbers not known before a certain point in time. Third, this proof can be presented offline and at any point in the future. For example, the proof could be mailed to a trusted third party, encrypted and signed by an application, only to be opened if needed and authorized. |
| Gilles Pütz  
*University of Geneva* | Measurement dependent locality | I will present the concept of measurement dependent locality (MDL), an idea which arises naturally when considering the possibility that the measurement choice in an experiment may be influenced by an adversary. I will show that quantum mechanics resists arbitrary lack of measurement dependence already in the simplest nonlocality scenario. If time permits, I will also introduce the idea of limited detection locality (LDL) and present a link between MDL and LDL. |
| Bing Qi  
*Oak Ridge National Laboratory* | Towards practical quantum key distribution using untrusted devices | I will discuss practical issues in the implementation of measurement-device-independent quantum key distribution (MDI-QKD), including both discrete variable protocol based on single photon detection and continuous variable protocol based on coherent detection. I will also make a comparison between MDI-QKD and other related protocols, such as the conventional BB84 QKD with four state modulation and the recently proposed detector-device-independent (DDI) QKD. |
Mohsen Razavi  
*University of Leeds*

Recent progress in memory-assisted measurement-device-independent QKD

I will discuss the recent theoretical developments with memory-assisted MDI-QKD. We previously showed that in order to beat existing no-memory QKD systems, in terms of rate-versus-distance behavior we either need a single-atom-like memory, or nearly ideal EPR sources. After reviewing the previous results, I will discuss the potential of nitrogen vacancy centers, in the former scenario, and that of quantum dot sources, in the latter. I will identify the gap between the current technology and what is needed to go beyond the Takeoka-Guha-Wilde bound.

Valerio Scarani  
*National University of Singapore*

A primer on device-independent self-testing

The words "self-testing" refer to the possibility that a device emits information that allows monitoring its internal status. These words were used in quantum information by Mayers and Yao to describe a remarkable possibility: that the quantum state and measurements being used in some black boxes be revealed by simply looking at the input-output statistics. In this talk, I'll review the status of this research field: states that can in principle be self-tested, robustness of the assessment, and of course many open questions.

Marco Tomamichel  
*University of Sydney*

Are current security proofs of quantum cryptography trustworthy?

I will report on recent work with Anthony Leverrier, where we try to prove security for ordinary, device-dependent cryptography schemes in the most rigorous way possible. We find that it is important to accurately model finite size effects and all the random seeds and communication transcripts that arise in a protocol. We hope that the framework we introduce will help bridge the gap between theory and practice in quantum cryptography since it makes explicit all the assumptions that go into a security proof.

Philip Walther  
*University of Vienna*

Quantum Photonics Technology for Secure (Cloud) Quantum Computing

The advantages of the photons makes optical quantum system ideally suited for a variety of applications in quantum information processing. Here I will review results for the realization of secure quantum cloud computing, where quantum information is securely communicated and computed. Related to secure measurement-based quantum computing I will also present a simplified experimental realization as well as the verification of quantum computing. As outlook I will discuss the current status of new quantum technology for improving the scalability of photonic quantum systems by using integrated circuits, superconducting single-photon detectors and novel photon sources.

Stephanie Wehner  
*Delft University of Technology*

Understanding nature from experimental observations: a theory independent test for gravitational decoherence

Quantum mechanics and the theory of gravity are presently not compatible. A particular question is whether gravity causes decoherence - an unavoidable source of noise. Several models for gravitational decoherence have been proposed, not all of which can be described quantum mechanically. In parallel, several experiments have been proposed to test some of these models, where the data obtained by such experiments is analyzed assuming quantum mechanics. Since we may need to modify quantum mechanics to account for gravity, however, one may question the validity of using quantum mechanics as a calculational tool to draw conclusions from experiments concerning gravity.

Here we propose an experiment to estimate gravitational decoherence whose conclusions hold even if quantum mechanics would need to be modified. We first establish a general information-theoretic notion of decoherence which reduces to the standard measure within quantum mechanics. Second, drawing on ideas from quantum information, we propose a very general experiment that allows us to obtain a quantitative estimate of decoherence of any physical process for any physical theory satisfying only very mild conditions. Finally, we propose a concrete experiment using optomechanics to estimate gravitational decoherence in any such theory, including quantum mechanics as a special case.

Our work raises the interesting question whether other properties of nature could similarly be established from experimental observations alone - that is, without already having a rather well formed theory of nature like quantum mechanics to make sense of experimental data.
| Xiaodi Wu  
(Massachusetts Institute of Technology) | New results on randomness extraction in the presence of quantum side information | In this talk, I will report our recent results on quantum-proof seeded and multi-source randomness extractors.  
1) Firstly, I will talk about a new construction of quantum seeded extractors that is optimal for min-entropy sources of inverse polynomial entropy rate, i.e., for any length n source with k=n^c min-entropy, 0 < c < 1. This is a strict improvement over existing constructions of quantum seeded extractors, such as Trevisian’s extractor and (almost) pair-wise hashing.  
2) Secondly, I will show that all classical multi-source extractors can either directly work, or be modified to work in the so-called general entangled (GE) side information model at the cost of one extra random source. The GE model is a unification and generalization of the only existing side information models for multi-source randomness extraction proposed by Kempe & Kasher. Our constructions essentially match the best known constructions of classical multi-source extractors. |
|---|---|---|
| Qiang Zhang  
(University of Science and Technology of China) | Recent experimental progress in QKD with realistic devices | I will discuss the recent experimental development in measurement device independent QKD, free space QKD with strong sunlight background and QKD with a QBER of 29%. |