Preliminary Study On A Sasaki-Yamamoto-Koashi-like Quantum Key Distribution Scheme

H. F. Chau
Department of Physics, University of Hong Kong

Abstract

Sasaki, Yamamoto and Koashi recently discovered a novel quantum key distribution scheme that only requires to estimate the error rate measured in one basis. However, their scheme is not very practical mostly because no one knows how to efficiently prepare the initial states needed in standard quantum optics setups. Here I report a variation of their scheme that partly solved the state preparation problem. I also report a preliminary analysis of the unconditional security of this scheme.

The early part of this work is done in collaboration with my former postdoc C.-H. F. Fung.

Quantum Effects in Unambiguous Communication

Runyao Duan
University of Technology Sydney, Australia

Abstract

We study the possibility of communicating classical information unambiguously with noisy quantum channels where the receiver can either correctly recover the classical message sent by the sender or simply claim an uncertain outcome. A notion of unambiguous capacity is introduced to characterize the optimal communication rates one can achieve under unambiguous decoding strategies. We provide a necessary and sufficient condition for the feasibility of unambiguous communication by establishing a connection to the extendibility of Kraus operator space of quantum channels. Consequently, we show that unambiguous capacity can be super-activated: there are two quantum channels both having zero unambiguous capacity can be used jointly to send classical information unambiguously. Finally, we find auxiliary resources such as shared entanglement, classical feedback, or quantum feedback, can considerably improve the unambiguous capacity to achieve the ordinary (small-error) capacity.

Replicating the Benefits of Closed Timelike Curves without Breaking Causality

Mile Gu
Tsinghua University

Abstract
In general relativity, closed timelike curves can break causality with remarkable and unsettling consequences. At the classical level, they induce causal paradoxes disturbing enough to motivate conjectures that explicitly prevent their existence. At the quantum level, resolving such paradoxes induce radical benefits - from cloning unknown quantum states to solving problems intractable to quantum computers. Instinctively, one expects these benefits to vanish if causality is respected.
In this talk, we show that in harnessing entanglement, we can efficiently solve NP-complete problems and clone arbitrary quantum states - even when all time-travelling systems are completely isolated from the past. Thus, the many defining benefits of closed timelike curves can still be harnessed, even when causality is preserved. Our results unveil the subtle interplay between entanglement and general relativity, and significantly improve the potential of probing the radical effects that may exist at the interface between relativity and quantum theory.

Maximal Privacy without Coherence

Debbie Leung
University of Waterloo

Abstract
A coherently transmitted quantum state is inherently private. Remarkably, co-herent quantum communication is not a prerequisite for privacy: there are quantum channels that are too noisy to transmit any quantum information reliably that can nevertheless send private classical information. Here, we ask how much private classical information a channel can transmit if it has little quantum capacity. We present a class of channels with input dimension D, quantum capacity less than 1, and private capacity $1/2 \log D$. These channels asymptotically saturate an interesting inequality $P \leq (\log D + Q)/2$ for any channel where D is in the input dimension, P and Q are the private and quantum capacities respectively.

Co-author Ke Li, Graeme Smith, and John Smolin

Projection Methods in Quantum Information Science

Chi-Kwong Li
College of William and Mary

Abstract
We discuss how to use projection methods to solve problems arising in quantum information science.

Linear Optical Demonstration of Quantum Speed-up with a Single Qudit

Jian Li
Department of Physics, Southeast University

Abstract

Though quantum algorithms act as an important role in quantum computation science, not only for providing a great vision for solving classically unsolvable problems, but also due to the fact that it gives a potential way of understanding quantum physics, the origin of the power of quantum algorithm is still an open question. Thus realizing simple and intuitive quantum algorithms appears to be essential. We experimentally realize a quantum speed-up algorithm on four-level system with linear optical elements. This algorithm gives the parity of a permutation twice faster than the corresponding classical algorithm. Apart from speed-up, there is another fascinating feature of this algorithm, that no correlations are required. Our experiment shows that even a single pure qudit is sufficient to design an oracle-based algorithm which solves a black-box problem, demonstrates quantum speed-up over any classical approach to the same problem and proves contextuality plays an important role in the speed-up.

Co-author Xiang Zhan, Hao Qin, Zhi-hao Bian, and Peng Xue

Foiling Quantum Hackers

Hoi-Kwong Lo
University of Toronto

Abstract

In principle, quantum key distribution (QKD) offers unconditional security based on the laws of physics. In practice, recent activities in quantum hacking have highlighted the security loopholes in practical QKD systems. Fortunately, counter-measures against quantum hacking have emerged as a hot topic in QKD. In this talk, I will discuss how the legitimate users, Alice and Bob, could protect their QKD systems against both attacks on their sources and detectors. For detectors, I will review the recent development of measurement-device-independent quantum key distribution (MDI-QKD), which is automatically immune to all attacks on detectors. For sources, I will discuss about the recent proposal and experiment of a loss-tolerant protocol and how Alice and Bob could quantify the imperfections at sources and take them into account in the key rate formula. In summary, means to protect attacks on both sources and detectors are now available, thus paving the way to secure QKD against both types of attacks for the first time. This brings us one step closer to achieving the Holy Grail of communication security—unconditional security.

[References: See H.-K. Lo, M. Curty and K. Tamaki, (Invited Review), Nature Photonics, 8, 595604 (2014) and also http://arxiv.org/abs/1408.3667 and http://arxiv.org/abs/1409.5157]

Quantum Key Distribution with Discrete Phase Randomization

Xiongfeng Ma
Institute for Interdisciplinary Information Sciences, Tsinghua University

Abstract

Coherent state photon sources are widely used in quantum information processing. In many applications, the coherent state is functioned as a mixture of Fock states by assuming its phase is continuously randomized. In practice, such assumption cannot be satisfied perfectly. To bridge this gap, we show that a discrete phase randomized source can well approximate its continuous counterpart. As an application, we give security bounds for discrete phase QKD schemes, which can be easily realized in practice and our simulation shows that with only a small number (say, 10) of discrete phases, the performance of discrete phase randomization is very close to the continuous one.

Quantum Detection of Magnetic-field Gradient Using Entangled Atoms

Ho-Tsang Ng
Institute for Interdisciplinary Information Sciences, Tsinghua University

Abstract

Quantum sensing and metrology play an important role in science and engineering. For example, magnetic resonance imaging is important in medical imaging which requires an accurate estimation of magnetic field gradient. In this talk, I will discuss a method to detect the microwave magnetic-field gradient by using a pair of entangled atomic Bose-Einstein condensates [1]. We consider the two spatially separated condensates to be coupled to the two different magnetic fields. The precision of measurement can reach the Heisenberg limit. We find that the entangled atoms can outperform the uncorrelated atoms in probing the magnetic fields even in the presence of atom losses. We also briefly discuss to probe the magnetic-field gradient with a chain of atoms [2].

References:
[1] H. T. Ng, Phys. Rev. A 87, 043602 (2013).
[2] H.T. Ng and K. Kim, Optics Communications 331, 353 (2014).

Continuity of Quantum States of Maximum Entropy

Yiu Tung Poon
Iowa State University

Abstract

Given k observables $\mathbf{F} = \{F_1, F_2, \ldots, F_k\}$, the quantum convex support of $\mathbf{F}$ is

$$\mathbb{L}(\mathbf{F}) = \{\boldsymbol{\alpha} | \boldsymbol{\alpha} = (\mathrm{tr}\rho F_1, \ldots, \mathrm{tr}\rho F_k) \text{ for some quantum state } \rho\}$$

For $\boldsymbol{\alpha} \in \mathbb{L}(\mathbf{F})$, the set

$$\mathcal{L}(\boldsymbol{\alpha}) = \{\rho \,|\, \mathrm{tr}\rho F_i = \alpha_i,\ i = 1, \ldots, k\},$$

is called a linear family of quantum states. Let $\rho^*(\boldsymbol{\alpha})$ denotes the state in $\mathcal{L}(\boldsymbol{\alpha})$ with maximum entropy. We study the continuity of the maps $\boldsymbol{\alpha} \to \mathcal{L}(\boldsymbol{\alpha})$ and $\boldsymbol{\alpha} \to \rho^*(\boldsymbol{\alpha})$.

Quantum Error Correction without Error Syndrome Detection

Shiyu Shi
The Hong Kong Polytechnic University

Abstract

We know that Quantum Error Correction (QEC) usually takes the approach of encoding, error syndrome detection, error correction and decoding. Recently, a method of QEC without error syndrome detection was proposed by Li, Makahara, Poon, Sze, and Tomita. Based on this method, we give recovery circuits for [5,1,3] code and [8,3,3] code respectively and give an intuitive interpretation to the idea of recovery without error syndrome detection.

Quantum Walk, Potential Application and Physical Implementation

Jingbo Wang
School of Physics, The University of Western Australia

Abstract

Quantum walk represents a generalised version of the well-known classical random walk. Regardless of their apparent connection, the dynamics of a quantum walk is often non-intuitive and far deviate from its classical counterpart. A multi-particle quantum walk presents an even richer dynamical system due to intrinsic quantum correlation and interaction. Current research is suggesting potential applications across a wide range of different fields. In this talk, I will give a brief introduction to quantum walks, discuss their potential applications, and consider several physical implementation schemes.

Quantum Uncertainty and the Error-disturbance Tradeoff

Shengjun Wu
Nanjing University

Abstract

The indeterminacy of quantum mechanics is originally presented by Heisenberg through the tradeoff between the measuring error of the observable A and the consequential disturbance to the value of another observable B. The tradeoff now has become a popular interpretation of the uncertainty principle. However, the historic idea has never been exactly formulated previously and is recently called into question. A theory built upon operational and universal valid definitions of error and disturbance is expected to rigorously reexamine their relation. Here by putting forward such natural definitions, we demonstrate both theoretically and experimentally that, there is no tradeoff if the outcome of measuring B is more uncertain than that of A. Otherwise, the tradeoff will be switched on and well characterized by the Jensen-Shannon divergence.

Experimental Realization of Quantum Walks via Linear Optical Elements

Peng Xue
Department of Physics, Southeast University

Abstract

Emerging as the quantum analog of classical random walks (RWs), quantum walks (QWs) exhibit striking nonclassical properties and has drawn intense research interests in recent years with implications in various fields, for instance, quantum algorithm engineering, universal quantum computing, quantum simulation of physical system and important phenomena.

We implement a discrete QW with site-dependent single point phase defects with linear optics which is mainly a set of optical interferometers comprising beam displacers, wave plates and phase shifters. Single-photons created via type-I SPDC are chosen to be the walker which walks in its position space represented by longitudinal spatial modes implemented by beam displacers according to the polarization of photon. Wave plates are used to prepare the initial state and do the coin flipping. We introduce site-dependent phase defects to the QW which is realized by adding fully controllable polarization-independent phase shifters. With certain settings for phase shifters and coin-flip wave plates, the translational symmetry of an ideal standard QW is broken resulting in localization effect in a QW architecture. We investigate localization effect in the QW, including the positions of the localized single-photons and the strength of localization related to different site-dependent phase defects and coin settings. The effect would find applications in quantum algorithms and quantum state engineering. By introducing site-dependent coin operation we can also demonstrate an experimental implementation of unambiguous state discrimination of two equally probable single-qubit states via a one-dimensional photonic QW. Furthermore we experimentally realize a QW algorithm for implementing unambiguous state discrimination of two equally probable single-qubit states and symmetric informationally complete positive operator value measurement on a single qubit.

Besides, the versatility of our setup allows for extensions, such as the realization of multiparticle QWs, which would help to study the topological phenomena. Furthermore, the high-quality interferometer network can also be used in the field of optical quantum information processing.

Co-author Hao Qin, Zhihao Bian, Bao Tang, Xiang Zhan

Ultimate Precision Limit in Terms of Time-energy Cost

Haidong Yuan
Chinese University of Hong Kong

Abstract

Measurement and estimation of parameters are essential for science and engineering, where the main quest is to find out the highest achievable precision with given resources and design schemes that attain that precision. It is intuitive that the precision limit of measurement is bounded by time and energy: high precision usually requires more time and energy. I will present a framework which uses a quantification of a time-energy cost to compute the ultimate precision limit. This framework provides a clear physical picture for the ultimate precision limit and a systematical way of finding schemes that attain it. We further demonstrate the power of the framework by deriving asymptotically optimal feedback schemes and a universal time scaling for Hamiltonian parameter estimation.

Quantum Advantage in Playing Games

Shengyu Zhang
The Chinese University of Hong Kong

Abstract

In this talk, we will review recent advances of quantum game theory, with emphasis on advantages and limits of playing quantum strategies. In particular, we will exhibit some zero-sum games with fair Nash equilibria between two classical players, in which if one player changes to quantum, then she would have a significant advantage of winning the game. This quantum advantage exhits even when the Nash equilibria, as quantum states shared by two players, are not entangled or do not have positive discord. Future studies are called for on certain open questions.
