Abstracts

April 11, 2019 (Thu) [Afternoon Session]

13:00 – 13:50 Masahito Hayashi (Nagoya)

Title: Various security in quantum information

In this talk, I would like to present my seminal results in quantum security. My first study is quantum wire-tap channel. In this model, we assume two channels. One is the channel to the authorized receiver and the other is the channel to eavesdropper. In this problem, the code can be realized by the combination of hash function and error correcting code. Then, this idea has been applied to the security of quantum key distribution. Also, this approach as been applied to physical layer security, which is the classical setting. Secure satellite channel is an example of physical layer security.

Second, I discuss the verification of quantum computer. In the classical computer, the verification means the verification of the program. However, in the quantum case, there are two types of verification. One is the verification of the program for quantum computer. The other is the verification of the physically implemented hardware. I studied the latter topic. When we employ the measurement based quantum computation, this problem is reduced to the verification of quantum state. I have studied this topic in various settings. Finally, this idea has been applied to the verification of quantum supremacy.

13:50 – 14:30 Ximing Wang (SUSTech)

Title: Classification by Boosting – A Perspective with Quantum Advantage

In classical machine learning, a set of weak classifiers can be adaptively combined to form a strong classifier for improving the overall performance, a technique called boosting (e.g. AdaBoost). However, constructing the strong classifier for a large data set is typically resource consuming. Here we propose a quantum extension of AdaBoost, demonstrating a quantum algorithm that can output the optimal strong classifier with a quadratic speedup in the number of queries of the weak classifiers. Our results also include a generalization of the standard AdaBoost to the cases where the output of each classifier may be probabilistic even for the same input. We prove that the update rules and the query complexity of the non-deterministic classifiers are the same as those of deterministic classifiers, which may be of independent interest to the classical machine-learning community.

14:50 – 15:40 Harumichi Nishimura (Nagoya)

Title: Possibility of classical verification for quantum computation

Whether a server really does a task possible by a polynomial-time quantum computer for a client that can do only polynomial-time classical computation is an important open problem. Since this problem was recognized, there has been many studies that give partial solutions for this problem. In this talk, I will report some of the solutions, in particular, a solution in the case that the server is rational.

15:40 – 16:20 Seunghoan Song (Nagoya)

Title: Capacity of Quantum Private Information Retrieval with Multiple Servers

In this talk, I present a recent result on the capacity of quantum private information retrieval (QPIR) with multiple servers [arXiv:1903.10209]. In the QPIR problem with multiple servers, a user retrieves a classical file by downloading quantum systems from multiple servers each of which containing the whole classical file set, without revealing the identity of the retrieved file to any individual server. The QPIR capacity is defined as the maximum rate of the file size over the whole dimension of the downloaded quantum systems. Assuming the pre-existing entanglement among servers, we prove that the QPIR capacity with multiple servers is one regardlessly of the number of servers and files. We propose a rate-one protocol which can be implemented by using only two servers. This capacity-achieving protocol outperforms its classical counterpart in the sense of the capacity, server secrecy, and upload cost.

April 12, 2019 (Fri) [Morning Session]

09:20 – 10:10 Jacques Garrigue (Nagoya)

Title: Functional programming, type systems, proofs and models

In this talk I will attempt to present the relevant areas of my research. Namely:

- The OCaml programming language, its type system, and work on using it to handle linearity.
- Computer verified proofs of parts of the type inference algorithm.
- Proofs of programs, particularly succinct data structures and sum-product decoding.
- Formal proof of mathematical models: probabilities (with applications to information theory and possibly quantum programming)
- Formalization of convex and conical spaces, with applications to probabilistic programming.

10:10 – 11:00 Man-Hong Yung (SUSTech, Huawei)

Title: Quantum Computing for the Near Future

In the near future, it is possible that quantum devices with 50 or more high-quality qubits can be engineered. On one hand, these quantum devices could potentially perform specific computational tasks that cannot be simulated efficiently by classical computers. On the other hand, the number of qubits would not be enough for implementating textbook quantum algorithms. An immediate question is how one might exploit these near-term quantum devices for really useful tasks? In addition, one may also expect that these powerful quantum devices are accessible only through cloud services over the internet, which imposes the question of how might one verify the server, behind the internet, does own a quantum computer instead of a classical simulator? In this talk, I will share my thoughts over these questions based on my recent works.

11:00 – 11:50 Xingyao Wu (Huawei)

Title: Quantum Reinforcement Learning and Self-testing of Quantum Devices

In the reinforcement learning regime, the agent exchange information with the environment to learn its behavior so the final optimized strategy will give the best rewards. Although a lot results have been explored in the classical case, reinforcement learning in the quantum case has not been

studied too much so far. Here I will present our work that quantum agents can achieve exponential improvements in learning efficiency, surpassing previous results that showed only quadratic improvements. On the other hand, I will also present our previous works on self-testing quantum devices, where no assumption about the quantum devices need to be made (Hilbert space dimension, system mechanism, etc.)

April 12, 2019 (Fri) [Afternoon Session]

14:00 – 14:50 Francesco Buscemi (Nagoya)

Title: "Semiquantum games" to verify quantum correlations (in space and time)

In this talk I will first review the framework of "semiquantum nonlocal games," explaining its background (quantum statistical comparison) and its application (measurement-device-independent entanglement verification). I will then compare semiquantum nonlocal games with conventional (Bell) nonlocal games, showing, in particular, how semiquantum nonlocal games, contrarily to conventional nonlocal games, can be arranged in a time-like configuration without becoming trivial. This layout provides a very natural scenario to verify quantum correlations in time, with direct application to quantum channel/memory verification. I will conclude by highlighting the advantages of semiquantum games with respect to previous proposals.

14:50 – 15:30 Bin Cheng (SUSTech)

Title: Experimental Cryptographic Verification for Near-Term Quantum Cloud Computing

Recently, there are more and more organizations offering quantum-cloud services, where any client can access a quantum computer remotely through the internet. In the near future, these cloud servers may claim to offer quantum computing power out of reach of classical devices. An important task is to make sure that there is a real quantum computer running, instead of a simulation by a classical device. Here we explore the applicability of a cryptographic verification scheme that avoids the need of implementing a full quantum algorithm or requiring the clients to communicate with quantum resources. In this scheme, the client encodes a secret string in a scrambled IQP (instantaneous quantum polynomial) circuit sent to the quantum cloud in the form of classical message, and verify the computation by checking the probability bias of a class of output strings generated by the server. We provided a theoretical extension and implemented the scheme on a 5-qubit NMR quantum processor in the laboratory and a 5-qubit and 16-qubit processors of the IBM quantum cloud. We found that the experimental results of the NMR processor can be verified by the scheme with about 2.5% 2.5% 1.4% error, after noise compensation by standard techniques. However, the fidelity of the IBM quantum cloud is currently too low to pass the test (about 42% 42% 42% error). This verification scheme shall become practical when servers claim to offer quantum-computing resources that can achieve quantum supremacy.

15:50 – 16:30 Yuuya Yoshida (Nagoya)

Title: Asymptotic Properties for Quantum Dynamics

I talk about dynamics when a quantum channel is applied to an initial quantum state many times. More precisely, we discuss how the n-th iterated channel behaves asymptotically as n tends to infinity. Asymptotic decoupling is an asymptotic property on a bipartite quantum system, which

means that the n-th iterated channel breaks the correlation between two quantum systems as n tends to infinity. A goal of this talk is to clarify a necessary and sufficient condition that a tensor product quantum channel is asymptotically decoupling. For this goal, we introduce another asymptotic property, namely, mixing. Mixing asserts that the n-th iterated channel converges to a constant channel as n tends to infinity. By using this term, it turns out that asymptotic decoupling is equivalent to 'local' mixing.

16:30 – 17:10 Hayato Arai (Nagoya)

Title: Perfect Discrimination of Non-Orthogonal Separable Pure States on Bipartite System in General Probabilistic Theory

This talk addresses perfect discrimination of two separable states [arXiv:1903.01658]. When available states are restricted to separable states, we can theoretically consider a larger class of measurements than the class of measurements allowed in quantum theory. The pair of two classes of separable states and the extended measurements is a typical example of General Probabilistic Theories (GPTs). Moreover, the GPT, called SEP, is an example of a composite system of two quantum systems, which is different from our composite system. To separate our quantum theory from SEP, we consider perfect discrimination. First, we give a necessary and sufficient condition to discriminate two pure states perfectly in SEP. In particular, it reveals that SEP has perfect discrimination of two non-orthogonal pure states. Second, we consider the maximum number of states that are distinguishable simultaneously and perfectly, which is called capacity. In spite of the difference of discrimination of two pure states, the capacity in SEP is equal to that in quantum theory.