Abstracts.

11/5 (Tuesday)

佐々木 寿彦 （東京大学・光量子科学研究センター）
Title:Security proof of QKD as a combination of classical arguments: Based on the twin-field-type QKD
Abstract:Security proofs of quantum key distribution (QKD) protocols have to evaluate the finite-key effect rigorously in terms of quantum mechanics. We often decompose its evaluations into a combination of evaluations of the corresponding classical protocols that can be easily evaluated. In this talk, I will explain how this decomposition is justified, and what we have to pay attention to. As a example, I consider our recent work about a Twin-field-type QKD protocol. It is known as a protocol that makes the available distance of QKD almost twice without the quantum memory.

清水 俊也 （富士通研究所）
Title: Solving cryptographic problems using annealing computation
Abstract Studying the hardness of cryptographic problems with respect to various algorithms including quantum ones is a major problem. Recently, a computation method called annealing has attracted considerable interest in computer science. In general, this computation tries to minimize a specific type of polynomial called Hamiltonian, representing the Ising model. I introduce several methods of converting three kinds of cryptographic problems (RSA、MQ, lattice) to Hamiltonians and some experimental results.

山本 剛 （NEC）
Title:Quantum computing using superconducting circuits
Abstract:In this talk, I will explain some basic concepts and experimental techniques in superconducting quantum electronics assuming audiences from different fields and backgrounds. After introducing them, I will further discuss one of the important tools in the superconducting quantum circuit, a parametric amplifier, which is a microwave amplifier with almost quantum-limited noise performance. I briefly introduce the research activity on the development of the superconducting parametric amplifier, including our results, with some historical background and recent progresses.

11/6 (Wednesday)

Yan Bo Ti （University of Auckland）
Title:G2SIDH and their isogeny graphs
Abstract:In this talk, we will introduce G2SIDH and look at one aspect of the security of this system by considering the isogeny graph of principally polarised abelian surfaces. In particular, we will be examining the algorithms used in G2SIDH, and focus on the supersingular and superspecial principally polarised abelian surface isogeny graph. We examine potential attacks that exist due to the graph structures.

王 亜成 （東京大学）
Title:Algebraic cryptanalysis on multivariate cryptography
Abstract: With currently widely used cryptosystems, RSA and ECC, being threatened by the development of quantum computers because of Shor's factoring algorithm, research on the post-quantum cryptography has become more urgent. Multivariate cryptography, as one of the main candidates of post-quantum cryptography, uses a set of multivariate polynomials over a finite field as its public keys, and its security relies on the hardness of solving these public key polynomials. In this talk, I introduce methods for algebraically breaking a multivariate cryptosystem and explain their complexities. More specifically, I introduce solving the public key polynomials of a multivariate cryptosystem by directly computing its Grbner basis and explain its complexity. Then I introduce methods for remodeling the public key polynomials into a different polynomial system, then solve this new system by computing its Grbner basis.

木村 元 （芝浦工業大学）
Title:Quantum theory based on operational and informational viewpoints
— An informational origin for a distortion of the state space
Abstract: General probabilistic theory (GPT) is supposed to provide the most general framework for operationally well-defined probability, including both classical and quantum cases. In this talk, I will give a brief introduction to general probabilistic theories (GPTs) for application to quantum theory and quantum information theory. I also introduce our recent result of an informational characterization for a distortion of the state space. The result beautifully explains the reason why qubit, and only qubit, has a point symmetric state space (Bloch Ball).

鈴木 泰成 （NTT）
Title:Software infrastructure for experimental quantum error correction
Abstract:Quantum computer can solve problems such as factoring exponentially faster than classical ones. On the other hand, it is not straightforward to reliably scale it up to a useful size since error probabilities of quantum bits (qubits) are much larger than classical bits. The most promising way to solve this problem is to perform quantum error correction and decrease effective error probabilities to an arbitrary small value. Thus, many groups have made efforts to demonstrate high-performance and scalable quantum error correction. In order to practically improve error probabilities with quantum error correction, we need not only many qubits with small errors but also fast and near-optimal control software and algorithms for it. In this talk, I will discuss what is required for developing fault-tolerant quantum computer and show my recent results about software infrastructure for achieving practical quantum error correction.

Rudy Raymond （IBM 東京基礎研究所）
Title:Distributed average computation with near-term quantum devices for collaborative learning

Abstract:The task in computing average of datasets distributed across a network is fundamental in collaborative learning because the average can be used for many applications in decision making and decentralized controls. One of important aspects in such task is the requirement to compute the average without revealing each unique data own by a party in the network. Such task is traditionally solved with secure multiparty communication or average consensus protocols. However, such protocols often exploit homomorphic encryption which can be very limiting in practice. A recent work by Ide et al. (IJCAI 2019) shows how to securely and efficiently compute the average consensus without homomorphic encryption. Here, we show a quantum protocol to compute the average on near-term quantum devices that consist of at most 2 quantum bits and 1 quantum bit communication resources. This is a joint work with Tsuyoshi Ide of IBM T. J. Watson Research Center

11/7 (Thursday)

小柴 健史 （早稲田大学）
Title: On public verifiability of secure delegated quantum computation
Abstract: Secure delegated quantum computation (SDQC) is a protocol between a client Alice and a server Bob. Alice would like Bob to delegate her task to evaluate a function on her input with a quantum algorithm for the evaluation. As a security requirement, Alice does not reveal her input/output and even her algorithm to Bob. It is known that SDQC is possible in the unconditional setting and many protocols have been proposed in the literature. On the other hand, Bob might deviate from the protocol specification. Nonetheless, Bob may claim that he competes his task as required. Verifiability guarantees that such an illegal behavior by Bob can be detected by Alice. Alice can notice Bob ’ s dishonesty but it is difficult to prove Bob’s dishonesty. To resolve this problem, the notion of public verifiability would be important. In this talk, we will discuss possibilities and limitations of public verifiability of SDQC.

水谷 明博 （三菱電機）
Title:Security of QKD under pulse correlations in terms of key information
Abstract:To guarantee the security of QKD, we need to assume mathematical models on users ’ devices. They must incorporate physical properties of actual devices, otherwise the security of actual QKD system cannot be guaranteed. One of the actual imperfections of light sources, which have not been taken into account in the previous security poofs so far, is pulse correlations of key information among emitted pulses. In this talk, we present a general method to prove the security under these correlations.