論 文 の 内 容 の 要 旨

論文題目　Digital Quantum Information Processing with Continuous-Variable Systems
（連続変量系を用いた離散的量子情報処理）

氏　　名　　松浦　孝弥

Quantum continuous-variable systems are quantum systems characterized by physical quantities that can take continuous values. It appears in many physical systems, such as the position and momentum of oscillator modes of trapped ions and the complex amplitude of an optical mode. Especially, the quantum optical system is one of the most important continuous-variable systems for the quantum information application since light is a good information carrier for telecommunication and behaves quantum mechanically even in the room-temperature environment. Furthermore, the complex amplitude of the optical mode can easily be manipulated. However, using a quantum continuous variable as it is does not work in quantum information processing since a continuous variable is subject to continuous noises in the physical world, and such noises cannot completely be corrected. In order to perform reliable and fault-tolerant quantum information processing, information should be encoded in a digitized degree of freedom. In this thesis, digital quantum information processing with continuous-variables systems is studied in the quantum key distribution (QKD) and the quantum computation (QC), two major fields of quantum information processing.

For the QKD, the so-called continuous-variable QKD protocols, in which information is encoded on the complex amplitude of an optical pulse and the homodyne or heterodyne detector is used to measure it, are studied. More specifically, a continuous-variable QKD protocol that uses discretely modulated signals and the classical digital information processing is developed, and its security proof against general attacks in the finite-key case is established. This is

achieved by virtually introducing the discrete-variable quantum system into the continuous-variable system, and thereby reducing the security argument to that of discrete-variable QKDs, which is more mature. This is in sharp contrast to the previous security analyses on this kind of QKD protocol, where they directly use continuous variables in the security analyses and thus have difficulty in extending them to the finite-key case. Another key to our security proof is the development of the method of estimating a lower bound on the fidelity to the coherent states, which eventually leads to the evaluation of how well the discrete-variable system can be approximated by the continuous-variable one. These security analyses are further elaborated, and a protocol whose key rate against the loss noise achieves almost optimal scaling is obtained.

For the QC with the continuous-variable system, the Gottesman-Kitaev-Preskill (GKP) code, which encodes discrete quantum information into a continuous-variable system, is studied. This code has many desirable properties for the optical implementation of QC; e.g., the universal QC is possible using only the Gaussian operations on the encoded states, which are relatively easy to implement in the quantum optical system. Because the ideal GKP-encoded state is unphysical and thus only its approximation in some sense is realizable, several approximations have been developed since the first proposal of the GKP code. In this thesis, these conventionally used approximations are shown to be equivalent and the explicit correspondences between the approximation parameters are given. This enables the direct comparison between the previous researches that are based on the different approximations. As the final result, an efficient method to implement the universal fault-tolerant QC using the Gaussian operations and only one type of the GKP-encoded state is developed. Contrary to the previous method that uses the probabilistic state conversion and the costly distillation, our method can prepare the necessary elements deterministically. Based on the previous proposals of generating approximate GKP-encoded states, the physical systems that are suitable for our method of realizing the universal QC are investigated.

The results in this thesis thus broaden the possibilities for reliable quantum information processing with continuous-variable systems.