論文の内容の要旨

APPLICATION OF FORMAL METHODS TO QUANTUM CRYPTOGRAPHY
(形式的手法の量子暗号への応用)

氏名　久保田　貴大

In general, it is difficult to verify security of cryptographic protocols. Indeed, flaws of designs and security proofs of some protocols were found after they had been presented. In verification using formal methods, protocols and security properties are described in formal languages, and correctness of designs and security proofs are deduced by inference rules. While a number of formal frameworks and verification tools have been developed and applied to classical protocols, few formal methods have been applied to security proofs of quantum protocols. The contributions of this thesis consist of the following three results.

First, we developed a software tool to verify the bisimulation relation of configurations (pairs of processes and quantum states) of qCCS, a quantum process calculus presented by Feng et al. Bisimilar configurations behave indistinguishably from the outside. We designed a formal framework for the verifier, which we call nondeterministic qCCS, on the basis of qCCS by Feng et al. While the transition system of qCCS is nondeterministic and probabilistic, we presented a nondeterministic and non-probabilistic transition system for configurations, extending the definition of them. This allows the verifier to verify bisimulation relation efficiently. Next, we designed the verifier to handle security parameters and quantum states symbolically. A purpose is to apply it to quantum cryptographic

protocols, where the dimensions of quantum states depend on security parameters. When the verifier checks bisimulation relation of configurations, it uses user-defined equations on the symbolic representations to check the quantum states that the outsider can access are always equal. Besides, the verifier is sound with respect to qCCS, that is, when it runs with two configurations as input and returns *true*, a symbol representing success of the verification, the configurations are in bisimulation relation in the qCCS's definition.

Second, we defined the notion of approximate bisimulation relation of configurations of nondeterministic qCCS. Approximately bisimilar configurations behave indistinguishably from the outside up to negligible probability. We then proved that the approximate bisimulation relation is closed under application of evaluation contexts of processes. This suggests sanity of our definition as well as feasibility in practice. As a result, we are able to formally verify not only that protocols are precisely equivalent but also that protocols are equivalent up to negligible probability. Moreover, we extended the verifier to verify the approximate bisimulation relation of configurations.

Third, we formally verified Shor and Preskill's security proof of BB84 quantum key distribution protocol. They first considered another protocol (the EDP-based protocol) and proved the security of BB84 and the EDP-based protocol is equivalent. They next proved the latter is secure. For the first step of their proof, we formalized the two protocols as configurations and formally verified that they are bisimilar. For the second step, we defined a completely secure protocol (EDPideal) and formally verified that the configurations of it and the EDP-based protocol are approximately bisimilar. This is the first work where a security proof of a quantum cryptographic protocol is mechanically verified using a software tool.