別紙４

報告番号	※　　第　　号

主　論　文　の　要　旨

論文題目　Information-Theoretic Aspects of Quantum Private Information Retrieval
(量子プライベート情報検索の情報理論的側面)

氏　　名　SONG Seunghoan

論　文　内　容　の　要　旨

When a user retrieves information from databases, it is often required to protect the privacy of the user. Quantum private information retrieval (QPIR) is a protocol in which a user retrieves one of f messages from non-communicating n servers by downloading quantum systems without revealing the identity of the retrieved message to any individual server. Symmetric QPIR is a QPIR with server secrecy in which the user obtains no information of non-targeted messages.

This thesis investigates the fundamental communication limit of the symmetric and non-symmetric QPIR and constructs the optimal QPIR protocols achieving the communication limit. The communication cost of a QPIR protocol is evaluated by the QPIR rate defined as the ratio of the size of one message to the whole dimension of the downloaded quantum systems. The supremum of the QPIR rate, called the QPIR capacity, characterizes the communication limit of QPIR.

Assuming that the servers share prior entanglement, we prove that the symmetric and non-symmetric QPIR capacities are 1 regardless of the number of servers and

messages. We construct a rate-one protocol only with two servers. This capacity-achieving protocol outperforms its classical counterpart in the sense of the capacity, server secrecy, and upload cost. The strong converse bound is derived concisely without using any secrecy condition. We also prove that the capacity of multi-round QPIR is 1.

As a variant of the QPIR with stronger security requirements, the t-private QPIR is a protocol in which the identity of the retrieved message is kept secret even if at most t servers may collude to reveal the identity. We prove that the symmetric and non-symmetric t-private QPIR capacities are $\min\{1, 2(\mathrm{n} - \mathrm{t})\}$ for any $1 \leq \mathrm{t} < \mathrm{n}$. We construct a capacity-achieving QPIR protocol by the stabilizer formalism and prove the optimality of our protocol. The proposed capacity is also greater than the classical counterpart.

Finally, we give a symmetric $(n-1)$-private QPIR protocol with bipartite entangled states. The protocol has the QPIR rate $\lfloor \mathrm{n}/2 \rfloor^{-1}$, which implies that it is capacity-achieving for even number of servers n. The protocol is practical since the bipartite entangled states are reliably generated with current quantum technology compared to the other entangled states.