論 文 の 内 容 の 要 旨

論文題目　A Study on Practical Information Retrieval Systems and Formalization of Their Security Models Considering Diverse Privacy Requirements
（多様なプライバシー要件を考慮した情報検索システムの効率化とその安全性モデルに関する研究）

氏　　名　　林田　淳一郎

With the spread of the Internet, there are more and more opportunities for people to search for information on databases. In addition, there are still many cases where information is leaked from databases due to the complexity of information retrieval systems. For the secure operation of such complex information retrieval systems, rigorous security notions that capture realistic attacks are required. In this thesis, we show two types of results on the security of information retrieval systems. Specifically, we deal with the security of information retrieval systems when the elements stored in the database are plaintexts and when they are encrypted.

First, we show the results of public-key encryption with keyword search (PEKS) in Chapters 3 and 4. PEKS allows us to perform a keyword search on encrypted data without decrypting ciphertexts. For the future practical use of PEKS, it is crucial to analyze the construction of PEKS schemes. In addition, it is also essential to add more functionalities to the PEKS schemes to support more applications. In doing so, it is necessary to formalize the security for more complex systems rigorously. In Chapter 3, we show the generic construction of an anonymous key-policy attribute-based encryption scheme from the PEKS scheme. In Chapter 4, we review the existing definitions of security against replayable chosen ciphertext attacks to provide more rigorous definitions of security and clarify the relationships among them.

Next, we show the results of private information retrieval (PIR) in Chapters 5 and 6. In these chapters, unlike the case of PEKS, we are considering a setting where the data is not encrypted. In such a setting, we may want to keep the contents of the client's query secret from the database server as a security requirement, and PIR allows us to do so. In Chapter

5, we introduce a new security notion called query indistinguishability for PIR schemes supporting basic range queries on one-dimensional databases and give constructions of the schemes satisfying query indistinguishability. In Chapter 6, we extend the result of Chapter 5 and construct the PIR scheme supporting multi-dimensional range queries. This concept of query indistinguishability can be applied to schemes that support more complex queries and is essential when considering the practical use of PIR.

Even though information retrieval systems have become more complex, the elements stored in the database are basically classified into plaintext or encrypted cases. Therefore, this research is expected to become a foundation of the security of information retrieval systems that will become more complex in the future.