論 文 の 内 容 の 要 旨

論 文 題 目　Provable Security of Applied Public Key Cryptosystems and Heuristically Secure Protocols
（高機能公開鍵暗号技術と経験的なセキュリティプロトコルの証明可能安全性）

氏 名　大畑　幸矢

The information on the internet is always exposed the threat of eavesdropping and falsification. Even in these conditions, we can ensure the confidentiality and integrity of information by using cryptosystems. In the research of cryptosystems, especially in public key cryptosystems, it is strongly required that we should rigorously prove its security. When we prove the security of cryptosystems, we usually reduce its security to the difficulty of mathematical problems. In this framework, we can objectively judge the security. Although not all the cryptosystems without security proof are insecure, the concept of provable security is useful in many aspects. In this thesis, we show two types of results related to the provable security.

First, we denote the results of provably secure applied cryptosystems in Chapters 3-5. In general, it often appears many entities, keys, and ciphertexts in applied cryptosystems. Therefore, we have to consider a complex model to deal with various attacks. If we fail this modeling, it is meaningless to prove the security. In these chapters, we show the results about threshold public key encryption and proxy re-encryption under the extended models and security definitions. In Chapter 3, we show three new constructions of threshold public key encryption schemes with key re-splittability. In Chapter 4, we show a generic construction of a proxy re-encryption scheme with new functionality called re-encryption verifiability. In Chapter 5, we show a construction of a multi-hop and uni-directional proxy re-encryption scheme based on a cryptographic obfuscator. In this thesis, we discuss the practical / theoretical meaning of new models and security definitions.

Next, in Chapter 6, we extend the provable security to the security protocols other than cryptosystems. More concretely, this is a result about a protocol that we call “password reset protocol”. We define models and security definitions, propose generic constructions, prove its security, and implement a prototype to evaluate its efficiency. This result can improve the security of real world protocols. Moreover, we can expect progress of theoretical analysis for password reset protocol based on this result.