論文の内容の要旨

論文題目　Computationally Sound Formal Models for Cryptographic Protocols
(暗号プロトコルの計算論的に健全な形式的モデル)

氏名　　川本　裕輔

Formal and *computational* approaches have developed independently to verify the security of cryptographic protocols. In the formal approach, messages are abstracted into symbolic expressions, and attackers are allowed to perform only a fixed set of algebraic operations on symbolic expressions. The protocol verification in the formal approach is simple to automate, while it might miss some attacks. In the computational approach, messages are bit strings and attackers are probabilistic polynomial-time Turing machines. Protocol verification in the computational approach does not miss any attacks, while it is very complex and error-prone, as it is based on the computational complexity theory.

In recent years, many researches have shown the *computational soundness* of the formal approach: formal verification of protocols does not miss any attacks, provided that the cryptographic primitives used in the protocols satisfy certain security properties based on the computational complexity theory.

The purpose of the thesis is to provide the formal models for analyzing protocols that employ cryptographic primitives with security properties weaker or more realistic than those assumed in the previous studies, and to show the computational soundness of the formal models. The contribution consists of the following three soundness results.

The first is a soundness result for equivalence properties in the presence of a restricted attacker. We provide a formal model for a rerandomizable public-key encryption scheme, and show the computational soundness of the pattern-equivalence in the formal model, which enables us to analyze a mixnet protocol. This is the first work that provides a computationally sound formal model for a rerandomizable encryption scheme, which satisfies a security property weaker than the IND-CCA2 security. To prove the soundness, we introduce a novel method of dealing with composed randomnesses in patterns.

The second is a soundness result for trace properties in the presence of a fully active attacker. We provide a formal model for a ring signature scheme, and show the mapping lemma for the model, which implies the soundness of trace properties. This is the first work that provides a computationally sound formal model for a ring signature scheme. The most important contribution is to introduce a deduction rule for the rerandomization of signatures, which gives more power to the attacker in the formal model, so that we obtain the soundness result.

The last is a soundness result for equivalence properties in the presence of a fully active attacker and an unbounded number of sessions. We provide the applied pi-calculus for a public-key encryption scheme, a ring signature scheme, and a hash function, and show the soundness of observational equivalence between two processes. With these cryptographic primitives, there has been no soundness result for equivalence properties in the presence of a fully active attacker. Unlike the previous studies on computational soundness, this work covers a larger class of protocols, including negative tests and nests of process replications. The most significant contribution is that the soundness proof does not use a *computable parsing function* from bit strings to terms. This is a major difference from all existing studies on computational soundness. It allows us to deal with more cryptographic primitives, for instance, a *preimage-resistant and collision-resistant hash function*, for which the soundness of process calculi cannot be obtained by a proof with a computable parsing function that has been used in previous studies. Furthermore, the new proof method enables us to deal with the case where each signature bit string for a message is not necessarily appended with the message.