論文の内容の要旨

Efficiency Enhancement of Secure Multi-Party Protocols for Privacy and Privilege Protection
(プライバシーと権限を守るための安全な多者間プロトコルの効率化に関する研究)

古川 潤

Secure multi-party protocols are cryptographic protocols which multiple players engage in. Many application specific multi-party protocols have been proposed, which include electronic voting, electronic cash, electronic auction, broadcast encryption, traitor tracing, anonymous authentication, group signature, secret sharing, conference (group) key distribution, group key generation, etc. These multi-party protocols are designed mainly so as to carry out social activities in the network. The technique of general multi-party computation that enables multi-party to securely compute any efficient function is known. However, its results are mostly far from practical efficiency in the sense of computational, communication, and round complexity. This is the major reason why a large number of specific constructions of multi-party protocols has been proposed. Since a multiple number of players engage in multi-party protocols, they often have complex security requirements. Such circumstance, besides the fact that the number of players itself is large, makes it hard to construct efficient multi-party protocols. Thus, efficiency enhancement is the major and crucial interest in these designing of multi-party protocols. Among these examples of multi-party protocols presented above, electronic voting, broadcast encryption, and group signature can be listed as most useful multi-party protocols. This dissertation presents several efficiency enhanced variants of these protocols. They are an efficient publicly verifiable shuffle scheme, an efficient publicly verifiable shuffle and decryption scheme, an efficient publicly verifiable hybrid mix-net scheme, an aggregate shuffle argument scheme, an efficient compiler from Σ -protocol to deniable zero-knowledge argument, a black-box traitor revocable broadcast encryption scheme, a group signature scheme for separate and distributed authorities, and an efficient group signature based on bilinear mappings. These protocols are efficient enough for practical purposes.