論 文 の 内 容 の 要 旨

Encryption-based Privacy Preserving Data Mining - Collusion Resistant Protocol and Clustering on Secure Networks
（暗号化に基づくプライバシー保護データマイニング―結託耐性プロトコルとセキュアネットワーク上のクラスタリング）

氏名　　楊　　斌

Privacy is an important issue when one wants to make use of data that involves individuals' sensitive information. Research on protecting the privacy of individuals and the confidentiality of data has received contributions from many fields, including computer science, statistics, economics, and social science. In particular, recent advances in the data mining field have lead to increased concerns about privacy. In this thesis, we therefore concentrate our attention on the topic of privacy-preserving data mining, especially on the technologies in encryption-based secure computation.

A variety of cryptographic protocols have been used in order to communicate among the different parties, so that secure function computation is possible without revealing sensitive information of any party. Unfortunately, all these existing methods do not deal with the collusion problem. We propose a collusion-resistant secure computation protocol that can be applied in most privacy-preserving data mining algorithms.

In this thesis, we also consider the distributed data in secure networks, in which each record is regarded as an individual party. Under this assumption, we focus on the privacy-preserving clustering, and propose a Gibbs sampling method and an EM algorithm to privately perform the clustering for the network data.