2012 年度 HPCI セミナー
東京大学大学院新領域創成科学研究科「情報生命科学特別講義 II」

第 2 回 2012 年 10 月 19 日（金）14:50 ~ 15:40

Privacy-preserving search for chemical compound databases based on additive homomorphic encryption

加法準同型暗号を用いた化合物データベースのプライバシ保護検索

Kana Shimizu / 清水 佳奈
Computational Biology Research Center (CBRC)
National Institute of Advanced Industrial Science and Technology (AIST)
産業技術総合研究所　生命情報工学研究センター

Searching similar compound from a database is among the most important approaches in the process of drug discovery. Since a query compound is an important starting point for a new drug, the query compound is usually treated as a secret information. The most popular method for a client to avoid information leakage is downloading whole database and using it in a closed network, however, this naive approach cannot be used if the database also want to keep its privacy. In this study, we address the problem of searching similar compounds in a database in privacy-preserving manner, and proposed a novel protocol which is efficient in both computational cost and communication size. We implemented our protocol and compared it to general purpose Multi party computation (MPC) on a simulated data set. We confirmed that the CPU time of the proposed protocol is around 1000 times faster than that of MPC. The protocol can be used for the database where data is represented as a bit-vector, therefore, we expect that our protocol will be applied for a wide range of problems.

Keywords: additive homomorphic encryption, Tversky index, chemical compound database