清华大学高等研究院
Institute for Advanced Study, Tsinghua University

密码学学术报告 Cryptology Seminars

Title: A brief survey on secure multiparty computation

Speaker: 刑朝平 教授（上海交通大学）

Time: 2019年10月15日（星期二）上午10点

Venue: 清华大学 高等研究院（科学馆）322报告厅

Abstract

Secure multiparty computation (MPC) was formally introduced by Andrew Yao in 1982 as secure computation between two parties. The two-party case was then generalized to multi-party by Goldreich et al. The computation is based on tools such as secret sharing of all the inputs, oblivious transfer, homomorphic encryption, and zero-knowledge proofs for ensuring that all parties behave correctly. Unlike traditional cryptographic schemes, the adversary in this model may be a participant of the computation. Therefore, a secure multi-party computation protocol must tolerate malicious behavior of participants. Over years, better multi-party schemes are proposed with regard to robustness and efficiency. MPC has wide applications in privacy preserving computation, such as decision making like voting, statistics computations. It enables to compute aggregate functions of private inputs, while hiding the inputs themselves. For example, it can be used for calculating statistics of customer data across many banks, or of patient data across many hospitals, while hiding everything except for the final desired output of the computation. In the application of voting, the identity of each individual and his/her vote can be hidden from anyone else, yet MPC ensures that each individual is able to verify that their votes are correctly recorded and contribute towards the final decision. In this talk, I will give a brief survey on secure multiparty computation