



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: Secure Multiparty Computation versus Secure Outsourcing

Speaker: Prof. Yvo Desmedt
(University of Texas at Dallas, USA)

Time: 2019年4月10日 (星期三) 上午10点

Venue: 清华大学 高等研究院 (科学馆) 322报告厅

Abstract

The lecture starts with explaining Secure Multi-Party Computation (MPC). Then we explain the rise of cloud storage, cloud computing and social networks. We regard it as a consequence of a failure in the design of adequate OS (operating systems). We survey some of the solutions proposed to address security problems on the cloud.

This presentation is focused on analyzing whether MPC is the correct technique for this problem. Moreover, besides issues as speed, we show that other problems pop up that are irrelevant in a typical MPC setting.

