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: **Efficient Fully Homomorphic Encryption Schemes**

Speaker: **Prof. Shuhong Gao**
(***Clemson University, USA***)

Time: 2019年5月15日（星期三）上午8:30

Venue: 清华大学 高等研究院（科学馆）322报告厅

Abstract

As cloud computing, internet of things (IoT) and blockchain technology become increasingly prevalent, there is an urgent need to protect the privacy of massive volumes of sensitive data collected or stored in distributed computer networks or cloud servers, as many of the networks or servers can be vulnerable to external and internal threats such as malicious hackers or curious insiders. The Holy-Grail of cryptography is to have practical fully homomorphic encryption (FHE) schemes that allow any third party (including cloud servers, hackers, miners or insiders) to perform searching or analytics of an arbitrary function on encrypted data without decryption, while no information on the original data is ever leaked. The breakthrough was made by Gentry in 2009 who discovered the first FHE scheme, and since then many improvements have been made on more efficient homomorphic encryption schemes. The main bottlenecks are in bootstrapping speed and large cipher expansion factor (the size ratio of ciphertexts over plaintexts): the current best FHE schemes can compute bootstrapping of one bit operation in a fraction of a second and have a cipher expansion factor of 8,000. In this talk, we present compact FHE schemes that achieve cipher expansion factor of 2.5 to 6 under secret key and 6.5 to 20 under public key while the bootstrapping speed matches the current best FHE schemes.