上海交通大学自动化系
Department of Automation
Shanghai Jiao Tong University

系统控制与信息处理教育部重点实验室
Key Laboratory of System Control and Information Processing, Ministry of Education

学术报告会

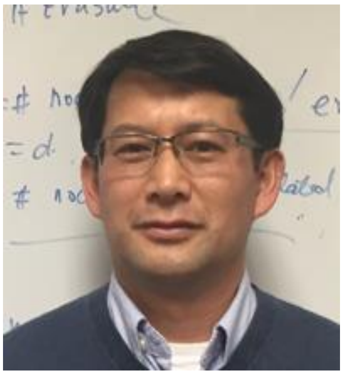
时　间：11月08日（周五）下午14：00-16：00

地　点：电信群楼2-406

Efficient Fully Homomorphic Encryption Schemes

Shuhong Gao

Clemson University



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 and get encrypted results, while no information on the original data or the results is ever leaked. Gentry in 2009 who discovered the first FHE scheme, and since then many improvements have been made on designing 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. The talk is based in part on joint work with Benjamin Case, Gengran Hu, and Qiuxia Xu.

Biography:

Shuhong Gao received his BS (1983) and MS (1986) from Department of Mathematics, Sichuan University, China, and PhD (1993) from Department of Combinatorics and Optimization, University of Waterloo, Canada. From 1993 to 1995, he was an NSERC Postdoctoral Fellow in Department of Computer Science, University of Toronto, Canada. He joined Clemson University in USA in 1995 as an assistant professor in Mathematical Sciences, and was promoted to associate professor in 2000 (with early tenure) and to full professor in 2002. Professor Gao's research interests include coding theory, cryptography, blockchains, symbolic computation, computational number theory and computational algebraic geometry. More information about his research and teaching can be found at Applicable Algebra Lab:
https://www.ces.clemson.edu/aca/.