NANYANG TECHNOLOGICAL UNIVERSITY

SEMINAR ANNOUNCEMENT

Lightweight Symmetric-Key Cryptography

Dr Guo Jian

Nanyang Technological University

Date: 12 July 2017 (Wednesday)
Time: 10.00am – 11.00am
Venue: MAS Executive Classroom 2, MAS-03-07
School of Physical and Mathematical Sciences

Abstract

Recent years have witnessed massive and wide deployment of IoT devices, ranging from smart cards to implanted medical devices. It is estimated that 50 billion IoT devices will be connected by year 2020. The diverse feature of IoT devices results in many special requirements to cryptographic mechanisms over traditional ones, such as low hardware area when implemented on small devices or low energy consumption when running on devices powered by limited battery. We show, by examples of concrete designs, how effective cryptographic mechanisms are still possible under these constraints without affecting the security strengths. It is also interesting to note that a single algorithm could be implemented in several ways to fit very different IoT usecase scenarios while keeping the functionality and security strength unaffected.

Speaker Biography

Dr. GUO Jian received his Bachelor and PhD degrees from Nanyang Technological University, Singapore in 2007 and 2011, respectively. He worked in Agency for Science, Technology, and Research (A*STAR) in Singapore for two and half years. Currently he is with Temasek Laboratories at NTU, as a Principal Investigator and Senior Research Scientist, leading a group of researchers on symmetric-key cryptography. His research interests focus on symmetric-key cryptography, especially analysis, design, and implementations of cryptographic hash functions, block ciphers, authenticated encryption schemes, and their applications such as message authentication codes.

Host: Division of Mathematical Sciences, School of Physical and Mathematical Sciences

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES
DIVISION OF MATHEMATICAL SCIENCES
SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371
TEL: +65 6513 7470