北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
前 沿 讲 座

An Introduction to the Impact of Quantum Computer to Symmetric-Key Cryptography

Prof. Guo Jian

School of Physical and Mathematical Sciences
Nanyang Technological University

Host: 刘天任 助理教授
2026年6月1日 星期一 3:00pm
静园五院204室

Abstract

In this talk, we will introduce the quantum algorithms that are used to re-evaluate the security strength of the current symmetric-key cryptography schemes. For the schemes that could be broken, we will then show the counter-measures, i.e., how the symmetric-key cryptography could become post-quantum.

The talk is suitable for audiences without background knowledge in either quantum algorithms or cryptography.

Biography

Dr. Guo Jian obtained his Bachelor in Computer Engineering and PhD in cryptography from Nanyang Technological University in Singapore, in 2007 and 2011, respectively. He is currently a tenured Associate Professor with NTU. His major research interest is symmetric-key cryptography. He co-designed PHOTON --- one of the ISO standards of lightweight hash functions, CLOC and SILC authenticated ciphers --- one of the third-round candidates of the CAESAR competition, as well as LED --- one of the lightest block ciphers suitable for constrained hardware. He has done some intensive cryptanalysis against various cryptographic primitives including the latest NIST hash function standard SHA-3 and AES, on which he and his team won several awards. Among others, he published more than 60 papers in conferences/workshops under the International Association for Cryptologic Research (IACR). He is a founding co-chair of ASK — the Asian workshop on Symmetric-Key cryptography. He served as a Program Co-Chair of Asiacrypt 2023, the General Co-Chair of Asiacrypt 2021 and FSE 2013, a Program Committee Member of FSE, Asiacrypt, Eurocrypt, Crypto, and ACM CCS constantly. He is the first elected Chinese director of IACR Board, the Vice-Chair of ASIACRYPT steering committee, and a member of the Security and Privacy Standards Technical Committee in Singapore acting as delegate of the International Standardization ISO/IEC JTC 1/SC 27. He also actively collaborates with industry in forms of being a consultant for multiple companies including Huawei and being the Principal Investigator for R&D projects with PayPal Inc. Within NTU, he also co-founded and has been a Director of the Master of Science in Cyber Security program.