QuanTalks

IISc Quantum Technologies Initiative (IQTI)
Seminar Series

Title
Extending the Range of Quantum Cryptography

Speaker
Dr. Andrew Shields, Toshiba Europe Ltd, Cambridge, UK.
andrew.shields@crl.toshiba.co.uk

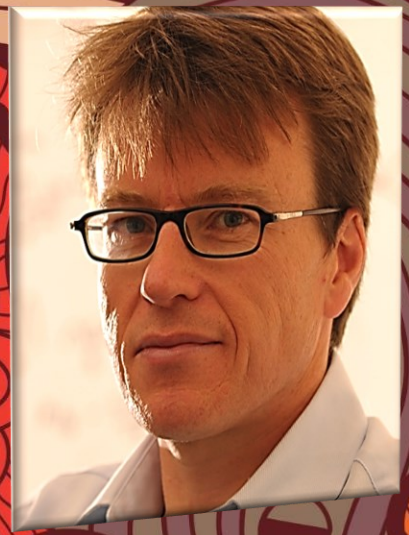
Date & Time
Wednesday, 22nd September
2021 at 5:00 PM IST

Abstract: Uniquely, quantum cryptography provides protocols whose security can be proven directly from information-theoretic principles and the laws of quantum physics, and which do not require any assumptions about the computational resources available to an adversary. Information-theoretic security will be important for data confidentiality in the future when we can expect more powerful computers and new algorithms to be at the fingertips of our digital foes. Of particular concern is the advent of quantum computer that can be used to launch efficient attacks on conventional techniques, such as the Diffie-Hellman key exchange algorithm.

In this talk I will review research at Toshiba in extending the limits of the technology, for example to high key rates[1], extending individual links beyond 500km [2,3] and operation on conventional data carrying fibres [5]. I will also discuss the commercialization of the technology in Toshiba and recent trials with lead customers.

References: [1] Yuan et al, J Lightwave Technology 36, 3427 (2018). [2] Lucamarini et al, Nature 557, 400 (2018). [3] Minder et al, Nature Photonics 13, 334 (2019). [4] Pittaluga et al, Nature Photonics 15, 530 (2021) [5] Dynes et al, Sci Rep 6, 35149 (2016).

Meeting Link
Click here to join the Meeting.



Biography : Andrew Shields leads R&D in Toshiba Europe on quantum technologies. According to Google Scholar, he has published over 500 research papers and patents in the field of quantum devices and systems, which have been cited over 22,000 times and has a Hirsch-index of >70. He has been involved in several large collaborative projects in Europe and is a member of the EU Strategic Research Agenda Working Group. He was a co-founder of the Industry Specification Group for QKD of ETSI and served as Chair for several years. He serves on the management team of the EU OpenQKD project and leads the AQuaSeC project developing next generation quantum communication technology.