Strategy and Synergy for Security

Society for Electronic Transactions and Security (SETS)

MGR Knowledge City, CIT Campus, Taramani, Chennai – 600113

www.setsindia.in

WEBINAR ON

QUANTUM COMMUNICATION

Date: 19th September 2020 (Saturday) **Time: 10:00am to 4.30pm**

Invited Talk 1 (Keynote Address)

Challenges and Opportunities in Building the Quantum Internet

by

Dr. Anil Prabhakar

Professor

Department of Electrical Engineering, IITM, Chennai

Abstract

The quantum internet is a vision for a new paradigm in secure communications that relies on the physics of quantum particles to ensure security. The many fields of classical communications, quantum optics, information theory, error coding, mixed signal electronics, fibre optic and free space optics, all come together under an interdisciplinary umbrella. There is the added challenge of standardization of communication equipment that will allow us to rapidly deploy and scale the network, while ensuring a high quality of service with complete security. This overview talk will attempt to place the ongoing efforts in India in context with similar developments happening worldwide. We will briefly describe the underlying technological needs, the collaborative efforts between academia, industry and research laboratories, and the challenges that we face in the physical and network layers. The quantum internet also enables new paradigms in quantum communications, and we will discuss opportunities for research, entrepreneurship and industry participation in the ongoing efforts.

Profile

Prof. Anil Prabhakar received his PhD in 1997 from Carnegie Mellon University, with a dissertation on the Nonlinear Spin-wave Optical Interactions. He has been with the faculty at the Dept. of Electrical Engineering, IIT-Madras since 2002, and is engaged across multiple laboratories that work on quantum optics, lasers and opto-fluidics. He is also a member of the Scientific Management Board for LIGO-India, to detect gravity waves, and the India-based Neutrino Observatory, and currently serves on the Editorial Boards for Scientific Reports (Nature) and the IEEE Transactions on Magnetics. Prof. Prabhakar's current research interests are in the areas of quantum technologies, with applications in sensing, communication and computing. As a Founder of QuNu Labs, incubated by IIT Madras, he focused on quantum key distribution (QKD). An earlier start-up, Unilumen Photonics that focused on fibre lasers was acquired by Jiva Sciences. He is currently the Director of Yali Mobility and Enability Foundation, companies that focus on rehabilitation engineering. He has over 50 research publications, and 13 patents on a wide range of devices in areas of photonics, magnonics and assistive devices.

Invited Talk 2:

Public Key Cryptography in a Quantum World

by

Dr. Prabha Mandayam
Assistant Professor
Department of Physics, IITM, Chennai

Abstract

Ever since the seminal discovery of the quantum factoring algorithm by Peter Shor in 94, there has been tremendous interest in developing public key exchange protocols that are secure against quantum adversaries. Quantum key distribution (QKD) provides a way by which classical keys can be encoded in quantum states and shared in a secure manner over public channels, with the promise of "unconditional" security based on the fundamental laws of quantum physics. Since the original QKD protocol due to Bennett and Brassard (BB'84) based on polarization-encoded photons, a variety of QKD protocols have been developed that invoke different quantum aspects of light such as entanglement (E'91 protocol), superposition (DPS-QKD) and quantum coherence (cow-qkd, twin-field qkd). In this talk we will briefly review these different approaches to QKD, compare their relative merits and security aspects. Finally, we will mention some important security loop-holes that arise in practical implementations and discuss two techniques - decoy states and measurement-device-independent QKD – which help to close the gap between theory and practice.

Profile

Dr Prabha Mandayam has received her PhD from Institute for Quantum Information, Caltech. She was a post-doctoral scholar with the Quantum Information group at the Institute of Mathematical Sciences and is currently an Assistant Professor in the Department of Physics at the IIT-Madras, working in the area of quantum information and quantum computing. Her research interests fall into three broad categories quantum error correction, quantum cryptography and quantum foundations.

Invited Talk 3:

Free Space Quantum Communication: The way forward to Satellite based Quantum Communication

by

Prof. Dr. R.P. Singh

Atomic, Molecular and Optical Physics Division,
Physical Research Laboratory, Ahmedabad

Abstract

Quantum key distribution (QKD) is perhaps the most remarkable application of quantum theory. It exploits the principles of quantum mechanics to enable secure exchange of information. QKD protocols allow two distant parties to share a secret random key. Once the key has been established, the two can exchange encrypted messages with the help of a one-time pad. BB84, the first QKD protocol, is proven to be unconditionally secure, based solely on the validity of the laws of quantum mechanics. It was later pointed out that imperfections in practical implementations seriously undermine the security of the QKD protocol. This resulted in several innovative protocols and proof of security with practical implementations. Notable among the proposed protocols was the decoy state protocol for its simpler implementation. In this method, the sender, prepares a set of decoy states in addition to the standard BB84 states. The decoy states in the form of coherent weak laser pulses are inserted randomly within the actual signal pulse train unknown to the receiver as well as to any potential eavesdropper. Without any prior knowledge regarding the position of the decoy pulses, there is an equal probability of eavesdropper attacking both the decoy as well as the BB84 signal pulses. By monitoring the quantum bit error rate (QBER) of the decoy pulses, sender and receiver can reliably estimate a lower bound for the secret key rate. We will see that using present technology, similar security with an increased key rate can be achieved without using decoy pulses. This is done utilising the inherent randomness in the number of photons per pulse of the source itself. We will also discuss the current international status of satellite based quantum communication and our efforts in this direction.

Profile

Prof. R.P. Singh did his M.Sc. in Physics from University of Allahabad and Ph.D. in Environmental Sciences from Jawaharlal Nehru University, New Delhi. After completing his Ph. D., he joined Prof. G.S. Agarwal as a post-doctoral fellow at University of Hyderabad and later as a faculty at Physical Research Laboratory, Ahmedabad. His areas of research include light scattering, phase singularities of light, nonlinear optics, quantum optics and quantum information.

Invited Talk 4:

A Frequency-Domain Approach to Quantum Key Distribution in Fibre-Optic Channels

by

Dr. K. Pradeep Kumar

Associate Professor, Department of Electrical Engineering, IIT Kanpur

Abstract

In this talk, I will describe our implementation of frequency-coded quantum key distribution (FC-QKD) over fibre-optic channels. In FC-QKD, bit to qubit mapping is achieved by mapping the prospective key bits onto the phase of the sidebands of the modulated optical carrier. At the receiver, the incoming optical signal—which includes sidebands and optical carrier—is modulated a second time with an independent phase derived from receiver's prospective key bit. The second modulation at the receiver effectively causes the sidebands to interfere constructively or destructively based on the choice of key bits of transmitter and receiver. A variety of optical modulators can be employed for this purpose. I will describe the QKD experiments that are currently being carried out in our lab at IIT Kanpur. I will discuss single-carrier and multi-carrier approaches towards FC-QKD and show that key rate can be increased by employing higher-order modulation and/or multi-carrier modulation. Decoy-state protocols help in pushing the key rate much higher than possible with non-decoy state protocols. I will also describe the supporting infrastructure such as random number generator, entangled-photon pair generation, single-photon detectors, and RF transceivers required to successfully implement FC-QKD systems over optical fibre channels.

Profile

Dr K Pradeep Kumar has received his PhD from Indian Institute of Technology, Madras on fibre based quantum key distribution. He is currently serving as an Associate Professor at Department of Electrical Engineering, IIT Kanpur. His current work is in the field of quantum cryptography, quantum optics for gravitational wave detectors, fibre-optic communications and photonics.

Talk 5:

Implementation Vulnerability Analysis of Quantum Cryptography

by

Mr Dillibabu S

Scientist, Hardware Security Research Team, SETS, Chennai

Abstract

Quantum cryptography relies on the Quantum uncertainty principle to achieve an information-theoretically secure system. Quantum Key Distribution (QKD) ensure un-conditional secrecy for cryptographic keys exchange between two parties. It also needs classical components such as a post-processing engine and an authentication module to minimize the loss. However, in general, naive implementations with practical imperfections might open loopholes, allowing an eavesdropper to compromise the security of a quantum cryptographic system. It has been happening for quantum key distribution (QKD). For instance, an authentication module, Wegman and Carter based polynomial hashing, Poly1305, adopted as the Message Authentication Code (MAC), was found to be vulnerable against the side-channel attacks. We share our efficient countermeasure techniques to thwart this kind of threat. Finally, we conclude with, how to implement a robust, reliable quantum key distribution system before field deployment.

Profile

Mr Dillibabu, works as a scientist at SETS. He completed his Bachelor of Engineering with specialization in Electronics and Communication Engineering under Anna University. His area of interest includes, Hardware Security, Quantum Communication, Light weight ciphers and post quantum cryptography.