WORKSHOP TITLE: QUANTUM CRYPTOGRAPHY FOR SECURE COMMUNICATION

Workshop Chair – Dr.V.Parthasarathy, sarathy.vp@gmail.com
Professor, Department of Computer Science and Engineering
Dean Research and Development
Vel Tech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, Tamilnadu, India.

Workshop Co-Chair – Dr.G.Murugaboopathi, gmurugaboopathi@gmail.com
Associate Professor, Department of Computer Science and Engineering, Kalasalingam University, Krishnankovil, Srivilliputtur (TK), Virudhunagar Dist, Tamilnadu, India.

Tutorial Syllabus **(6 Hour)**

Part A:

Introduction to Ensure Intercept and Resend Attack
Implementation of Quantum Cryptography and QKD
Practical limitations of QKD and its deployment
Security enrichment in QKD

Part B:

Users review on QKD
A review of recent trends and perspective

Quantum teleportation of optical coherent states demonstration

Part C:

Research design and methods
Surveys and questionnaire design
Methods of analysis
Impacts of QKD behavior studies

ABSTRACT

Quantum Cryptography uses the principles of Quantum Mechanics to implement a cryptographic system. The key problem is solved by using quantum techniques is that of eavesdropping detection. Quantum principles can be used to detect eavesdropping probabilistically when it occurs. The bits are represented as qubits, physically modeled by photons, and communicated over a quantum channel. **Quantum cryptography is a promising field with respect to the applications of the method and** the method itself combine several directions within natural science. If the presumption implied with total confidentiality. QKD offers unconditional security with the way the key distribution.

The process of QKD takes place in two stages involving the quantum channel and the classical channel. Our works mainly focus on the software development of the classical channel and to implement a prototype by modifying the existing 802.11 protocol that would use QKD to distribute key. However, the key exchanged in the existing protocol needs to be refreshed at regular intervals or upon requested by STA to maintain security of data. During the simulations, parity based bisect algorithm has been chosen as the reconciliation protocol. In comparison to other reconciliation protocols, the parity check method involves significant amount of processing cycles to observe the behavior under the worst possible conditions. The results prove that even under such extreme situations, the overall QKD protocol shows improved performances. Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of using the other complicated algorithms or technology.

Tutors' Recommendations

Participants are expected to actively contribute to in class discussions. All those participate will be awarded a *"Certificate of Participation*".

Workshop Fee: 100 EURO fee for professionals –50 EURO fee for students
Participants: Maximum number of participants is 30 individuals