Title: Secure Communication by Quantum Keys

Speaker: Prof. CM Chandrasekhar (IAP, IISc)

Abstract: The talk starts with the role of secure key generation in cryptography. Currently, RSA (a public-key cryptosystem) is the most widely employed for this. But, recent development in quantum computing renders it vulnerable to future quantum attacks. Hence, several candidates for secure key generation techniques have been proposed. Among them, BB84 is of special interest as it harnesses the power of quantum mechanics, making it relatively safe from Eve's droppers.

In the most generic cryptography protocol, the sender jumbles (encrypt) the message with a key. This jumbled message is sent to the intended receiver. Now, the receiver needs a key to decrypt the message. Thus, the secure generation and transmission of the key are of prime importance. The widely used RSA algorithm uses a public key to encrypt but a private key to decrypt. Both public (p) and private keys (q) are exactly two prime factors of some lengthy prime number (n). The security of RSA is due to computational difficulty in estimating p and q if n is provided. Recently a quantum algorithm by Shor has been proven to estimate keys p and q from n relatively faster.

Hence, we need to explore some other more secure protocols for key generation.

In 1984, Bennett and Brassard proposed a quantum mechanical way to generate keys (BB84). The security of this protocol relies on two quantum mechanical facts: (i) measuring a quantum state inherently changes it. (ii) Cloning a quantum state is impossible.

This protocol can be summarized in three steps as follow:

Step-I (Alice trials): Alice (sender) randomly chooses an orthonormal quantum basis {0, 1} or {+,- }. Then she sends a photon corresponding to the chosen basis.

Step-II (Bob trials): Bob (receiver) randomly chooses an orthonormal quantum basis {0, 1} or {+,- }. Then he measures the photon sent by Alice on that basis.

Step III: The above two steps are repeated several times. Then they classically communicate about which basis they had selected in a particular trial. But they don't share the measurement results. If, in a certain trial, their basis happens to be the same, then this information is sufficient for Alice to know what Bob has measured. Similarly, this is also sufficient for Bob to know what photon state has been sent by Alice. This is possible due unique property of orthogonal measurement in quantum mechanics. Now the set of successful trials can be used to make a key.

Entanglement based QKD as propesd by Ekert (1992) uses entangled qubits. Both particles are given one of the pair of entangled state. Measurement on entangled qubit is correlated. Hence, if they happen to choose a common basis of measurement then one can correctly predict what is corresponding measurement by the other.

Entangled photon pair is mostly by spontenous down conversion (SPDC) which obeys momentum and energy conservation rules. Entangled photons have several interesting utility like superdence coding where two bits of information can by sending single qubit.

The talks concludes with the scope to increase the speed of QKD by exploring higher dimensional quantum states.