Abstract:
The advancement in quantum computing, where Google, IBM, Microsoft, Intel are competing in the (exponentially growing) number of qubits in their (some already) commercial quantum computers that they produce, requires the reexamination of the Internet Security, and the public key infrastructure. The talk will describe the concept of overlay security together with blockchain-based directories for establishing symmetric keys. When combined with nested Lamport signature and Merkle trees for digital signatures the result is a complete, easily implementable architecture with information theoretically secure communication, and hash-based signatures.