Course Description

Course name	**#049 - Quantum vs Postquantum Cryptography**
Duration	**3 days**
Format	**Public Classroom, Inhouse Event and Online**

Overview

Research Professor Savo Glisic, Worcester Polytechnic Institute, MA, United States, is teaching this 3-day course about Quantum vs Postquantum Cryptography.

The research and practical results on Quantum computers in the recent years have given a major setback to classical and widely used cryptography schemes such as (Rivest-Shamir-Adleman) Algorithm and ECC (Elliptic Curve Cryptography). RSA and ECC depend on integer factorization problems and discrete logarithm problems respectively, which can be easily solved by Quantum Computers of sufficiently large size running the infamous Shor's Algorithm. Therefore, cryptography schemes which are difficult to solve in both traditional as well as Quantum Computers need to be evaluated. **This course provides a detailed survey on Post-Quantum Cryptography schemes and emphasizes their applicability to provide security in constrained devices.** A comprehensive insight is provided into the schemes which could possibly replace RSA and ECC for security in constrained devices.

Technical Focus

The research and practical results on Quantum computers in the recent years have given a major setback to classical and widely used cryptography schemes such as (Rivest-Shamir-Adleman) Algorithm and ECC (Elliptic Curve Cryptography). RSA and ECC depend on integer factorization problem and discrete logarithm problem respectively, which can be easily solved by Quantum Computers of sufficiently large size running the infamous Shor's Algorithm. Therefore, cryptography schemes which are difficult to solve in both traditional as well as Quantum Computers need to be evaluated. **This course provides a detailed survey on Post-Quantum Cryptography schemes and emphasizes their applicability to provide security in constrained devices.** A comprehensive insight is provided into the schemes which could possibly replace RSA and ECC for security in constrained devices.

While post-quantum cryptography is an effort to develop novel classical cryptosystems which are robust to factorization and other quantum algorithms, which is certainly one option, this does not completely solve the problem. The point is that there may be undiscovered quantum algorithms (or undiscovered classical ones) that might easily break the security of the new cryptosystems. In other words, postquantum cryptography is likely to offer only a partial and temporary solution to the problem. By contrast, quantum key distribution (QKD), discussed also in this course, offers the ultimate solution: restoring security and confidentiality by resorting to unbreakable principles of nature, such as the uncertainty principle or the monogamy of entanglement. **So, we cover in detail in this course the quantum cryptography as well.**

Even though QKD offers the ultimate solution to the security problem, its ideal implementation is hard to implement in practice and there are a number of open problems to be addressed. On one side, fully-device independent QKD protocols provide the highest level of quantum security, but they are quite demanding to realize and are characterized by extremely low secret key rates. On the other hand, more practical QKD protocols assume some level of trust in their devices, an assumption that allows them to achieve reasonable rates, but this also opens the possibility of dangerous side-channel attacks.

Besides a tradeoff between security and rate, there is also another important trade-off which is between rate and distance. Today, we know that there is a fundamental limit which restricts any point-to-point implementation of QKD. Given a lossy link with transmissivity, two parties cannot distribute more than the secret key capacity of the channel, which is i.e., scaling of secret bits per channel use at long distance. Ideal implementations of QKD protocols based on continuous-variable systems and Gaussian states may approach this capacity while those based on discrete variables falls below by additional factors. To overcome this limit and enable long-distance high-rate implementations of QKD, we need to develop quantum repeaters and quantum networks. In this way, we may achieve better long-distance scaling and further boost the rates by resorting to more complex routing strategies. The study of quantum repeaters and secure QKD networks is one of the hottest topics today which is also covered in this course. The course aims at providing an overview of the most important and most recent advances in the field of quantum cryptography, both theoretically and experimentally.

In near term, we expect that quantum security and QKD will be competing with so called post quantum security solutions and for this reason in a separate segment of this course we discuss in details pros and cons of each technology.

Who should attend?

Participants with background in either quantum physics, networks planning, design, deployment and control or networks/internet economics should benefit from participation. This includes researchers, students and professors in academia as well as industry, networks operators, regulators and managers in this field.

Course Daily Schedule

Monday

1. INTRODUCTION

Qubit
Entanglement
Quantum Gates and Quantum Computing
Quantum Teleportation and
Quantum Information Theory
Quantum algorithms
Quantum parallelism
Deutsch's algorithm
The Deutsch–Jozsa algorithm

2. QSA ALGORITHMS

The Deutsch Algorithm
Simon's Algorithm
Shor's Algorithm
Quantum Phase Estimation Algorithm
Grover's Quantum Search Algorithm
Dürr-Høyer Quantum Search Algorithm
Quantum Counting Algorithm
Quantum Genetic Algorithm
Harrow-Hassidim-Lloyd Algorithm
Quantum Mean Algorithm
Quantum Weighted Sum Algorithm

PHYSICS OF QUANTUM ALGORITHMS

Implementation of Deutsch's Algorithm
Implementation of Deutsch and Jozsa's Algorithm
Ethan Bernstein and Umesh Vazirani Implementation
Implementation of Quantum Fourier Transform
Estimating Arbitrary Phases
Improving success probability when estimating phases
The Order-Finding Problem
DESIGN EXAMPLE[1)]: How quantum parallelism and interference work
DESIGN EXAMPLE[2)]: Grover's algorithm
DESIGN EXAMPLE[3)]: Simon's
DESIGN EXAMPLE[4)]: Shor's Algorithm

Tuesday

3. POST-QUANTUM CRYPTOGRAPHY

3.1 Overview of Post-Quantum Cryptosystems
3.2 Rainbow

3.3 NTRU N-th degree Truncated polynomial Ring Units
3.4 LWE Cryptosystem
3.5 BLISS (Bimodal Lattice Signature Scheme (BLISS)
3.6 Variants of Merkle Signature Scheme
3.7 Lamport Signature
3.8 McEllice Cryptosystem: Code-based cryptography
3.9 Niederreiter Cryptosystem
Ex. 3.1 Key Generation for a SIS-Based Scheme

4. QUANTUM CRYPTOGRAPHY

4.1 Discrete Variable Protocols
4.2 Device-Independent QKD
4.3 Continuous-Variable QKD
4.4 Theoretical Models of Security
4.5 Limits of Point-to-Point QKD
4.6 QKD Against a Bounded Quantum Memory
Ex: Formulas for Gaussian states

Wednesday

5. QKD OVER SUBOPTICAL BANDS

Fundamentals of CVQKD
Security of CVQKD protocols
Composable security proof for cv QKD
Multicarrier Quadrature Division Modulation QKD over THz Band
TERAHERTZ QKD: System Model
Secret Key Rates
The total von Neumann entropy
System performance in the Extended Terahertz range

6. QUANTUM NETWORK PROTOCOLS

Summary of the analytical tools
Quantum states
Fidelity
Separable and entangled states
Quantum measurements
Quantum channel
LOCC channels
Quantum Link Layer Protocol
Entanglement swapping protocol
GHZ entanglement swapping protocol
Graph state distribution protocol
Entanglement distillation
Reinforcement Learning-based quantum decision processes
Quantum Networks
Tensor network

Reduced/marginal states of the overall quantum state of the network
Practical network architecture
Elementary link generation
Quantum memories
Examples of transmission channels that are relevant in practice
Imperfections
Ideal quantum state

Instructor Biography

Professor Savo Glisic. Worcester Polytechnic Institute, MA, United States.

He was Visiting Scientist at Cranfield Institute of Technology, Cranfield, U.K. (1976-1977) and University of California, San Diego (1986-1987). He has been active in the field of wireless communications for 30 years and has published a number of papers and books. The latest book "Advanced wireless Networks: 5G/6G joint design of technology and business models" by John Wiley & Sons, 2015, covers the enabling technologies for the definition of incoming 5G systems.

Dr. Glisic is running an extensive doctoral program in the field of wireless networking (www.telecomlab.oulu.fi/kurssit/networks/).

His research interest is in the area of network optimization theory, network topology control and graph theory, cognitive networks and game theory, radio resource management, QoS and queuing theory, networks information theory, protocol design, advanced routing and network coding, relaying, cellular, WLAN, ad hoc, sensor, active and bio inspired networks with emphasis on genetic algorithms and stochastic geometry. The latest interest is in the area of spectra sharing, robust heterogeneous network design, Artificial Intelligence (AI), Inter System Networking (ISN), block chains and complex networks theory. He is doing research within the WiFiUS collaborative program between the NSF in US and Finnish Academy as well as on a number of research projects sponsored by EU FP7 program. He is active within 5G ppp association preparing the projects for Horizon 2020 calls.

Dr. Glisic has served as the Technical Program Chairman of the third IEEE ISSSTA'94, the eighth IEEE PIMRC'97, and IEEE ICC'01. He was Director of IEEE ComSoc MD programs.

Dr. Glisic has been a member of the Continuing Education Institute-Europe faculty since 1995.