Quantum Readiness with Electi's Qu-R Framework ™

Executive Education Program

ELECTI Academy

Quantum Readiness with Electi's Qu-R Framework ™

About this course

In recent years there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems difficult or intractable for conventional computers. These mathematical algorithms are the backbone for the algorithms underpinning digital trust.

1. What the program covers

The program has been designed for enterprises and organizations interested in quantum computing. It presents the opportunities of quantum computing as well as associated challenges.

Upon completion of the course participants will be able to answer the following key questions:

- How can quantum computing affect our sector?
- What are the associated challenges?
- How can we anticipate these challenges?

The participants will be guided through **Electi's Qu-R Framework ™**, a proprietary analysis tool, that will help them evaluate the readiness level of their organization with respect to quantum computing security challenges.

Programs Available

Duration	1 Day
Price	TBD Euro + VAT
Material	Day 1 as described in Section 3. All materials are provided online on Electi Academy's Moodle Platform.

Duration	4 Days
Price	TBD Euro + VAT
Material	All days as described in Section 3. All materials are provided online on Electi Academy's Moodle Platform.

2. Who should take this course

The 1-day program is ideal for tech-savvy upper-management in enterprises and organizations that wish to familiarize themselves with quantum computing and the future impact it will have on a variety of industries. An overview of the evolution of quantum computing and the ramifications of recent advances are crucial for decision makers who would like to understand the risks posed by quantum computing attack scenarios.

The full 4-day program serves as an in-depth introduction to quantum computing with a particular emphasis on cryptography. This program is technical and is ideal for cryptographers, computer scientists and engineers as well as information security professionals.

3. What you will learn

Day 1 – Introduction to Quantum Computing

- What is quantum computing?
- Why does quantum computing matter?
- Introduction to quantum algorithms:
  - Shor's algorithm
  - Grover's algorithm
  - Bernstein–Vazirani algorithm
  - Quantum phase estimation algorithm
- What do the terms *quantum-safe*, *quantum-proof* and *quantum-resistant* mean?
- How quantum computing will revolutionize simulation, modelling, optimization & data processing
- Applications and impact on selected sectors: Healthcare, Military, Transportation, Banking, Internet-of-Things (IoT), Telecommunications, e-Commerce, Digital Assets
- Introduction to Electi's Qu-R Framework ™

Day 2 – InfoSec & Cryptography in the Post-Quantum Era (1)

- Information Security Requirements: *Confidentiality*, *Integrity*, *Authenticity*, *Non-Repudiation*
- Current cryptographic primitives
  - Symmetric Encryption
  - Asymmetric Encryption/PK Cryptography
  - Hash Functions
  - Digital Signatures
- How secure is Public Key (PK) Cryptography in the post-quantum era? Attacking computationally hard problems: Integer Factoring, Discrete Logarithm, ECDLP, etc.
- Classical Key Exchange Algorithms
- Potential attacks on existing PK Infrastructure and associated key exchange algorithms
- How can Symmetric Cryptography become quantum-resistant?
- Are hash functions secure in the post-quantum era?
- Challenges with Quantum Computing algorithms (large keys, large signature and messages size, computational efficiency)
- The notion of *Perfect Secrecy*

Day 3 – InfoSec & Cryptography in the Post-Quantum Era (2)

- Intractable problems in a post-quantum era
  - Lattice-based problems and the Shortest Vector Problem (SVP)
  - Multivariate Quadratic Equations
  - Syndrome Decoding Problem (SDP)
- Categories of post-quantum cryptographic algorithms
  - Lattice-based (NTRU, BLISS signatures)
  - Multivariate (Rainbow Signature Scheme)
  - Hash-based (Lamport signatures, Merkle signature scheme and the newer XMSS & SPHINCS schemes)
  - Code-based (error correcting code McEliece, Niederreiter, Goppa Codes)
  - Supersingular elliptic curve isogeny, symmetric key quantum resistance (AES, SNOW 3G)

Day 4 – Applications of Quantum Technology

- IT infrastructures in the post-quantum era
- The global quantum computing landscape
- The roadmap to standardization
- The NIST competition
- Electi's Qu-R Framework ™ Revisited

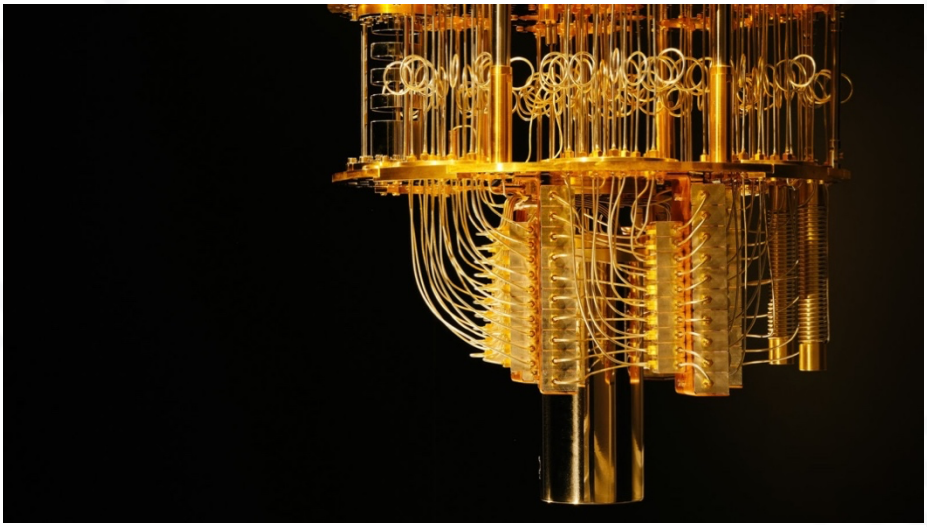
4. Whom you will learn from

Dr. Theodosis (Theo) Mourouzis is a cryptologist and information security professional. He holds a BA/MA in Mathematics and a MSc in Pure Mathematics from the University of Cambridge, a MRes in Security Science and a PhD in Information Security (Cryptography) from University College London. He was the first recipient in the UK Cyber Cipher Security Challenge in 2013. Theo is the Managing Director of Electi Consulting, a consultancy specialising in Blockchain, AI/ML and data science. He has published numerous scientific papers in the fields of cryptography and information security and has extensive experience in delivering training for organizations regarding these subjects. Dr. Mourouzis has worked with governments, multi-national companies and leading organisations such as Lloyd's Maritime Academy, Lloyds Bank, US Navy, Technology Strategy Board (TSB), Centre for Defence Enterprise (CDE), European Central Bank (ECB) and others. He is a PECB-certified ISO27001 Lead Implementer.

Mr. Alexandros (Alex) Hasikos is a cryptography expert and a blockchain engineer. He holds a BEng in Computer Systems Engineering from Brunel University, London and an MSc in Information Security from University College London. He is currently pursuing his PhD in Cryptography at UPF University in Barcelona. He is a partner and Head of Research and Development at Electi, a consultancy specializing in Blockchain, AI/ML and data science. Alexandros has extensive academic and worldwide industry experience and has published several research papers in the field of applied cryptography.

5. How you will learn

The content will be delivered in person via face-to-face lectures and demonstrations. Presentation slides, case studies and educational videos will also be provided. The course may require additional software and resources. Any additional requirements will be communicated to you upon registration and/or at the beginning of the course. All materials will be available online through Electi Academy's Moodle Platform.



A dilution refrigerator from an IBM quantum computer.
Photo: IBM Research

ELECTI
Academy

Executive Education

Contact Us: **academy@electi**consulting.com



contact

info@electiconsulting.com

visit

www.**electi**consulting.com