HellasQCI

Deploying advanced national QCI systems and networks in Greece

HellasQCI 1st Training Workshop report

18-19 21-22 September 2023, Athens, Greece

Lead beneficiary(s): GRNET
Author(s): Ilias Papastamatiou, Artemis Psarianou, Homer Papadopoulos
Date: September 26, 2023
Dissemination Level: Public

Abstract:
On September 18–19 and 21–22, 2023, at the National Technical University of Athens, Greece, the HellasQCI project held its first training session. With the aim of improving the security of sensitive data and important infrastructures in Greece and co-creating EuroQCI, the course was created to give participants theoretical and practical information on quantum communication.

The four-day event began with statements by Prof. Stefanos Kollias, Chairman of the Board of Directors of GRNET S.A., and was officially opened by Konstantinos Karantzalos, the new Secretary General of Telecommunications and Post. The keynote address was delivered by Dr. Eleni Diamanti, head of research at the CNRS at the Sorbonne University in Paris, on the topic of "Quantum Technologies - QKD Landscape in Europe."

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

Table of Contents

1. Report Analysis 3
2. Kick-off Photo material 7
3. Kick-off Media publications 11
4. Annex 1 – Full media publications (PDF) 12
5. Annex 2 – Kick-off agenda 13

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

1. Report Analysis

The HellasQCI project held its first training event on September 18-19 and 21-22, 2023, at the National Technical University of Athens, Greece.

The training was open to cybersecurity professionals, IT managers and engineers, security and IT experts, researchers, students, and practitioners in the field of quantum communication, as well as decision-makers interested in future-proofing their organisation's security infrastructure. Participants could attend in person or via livestream through the GRNET DIAVLOS service. The event had two different thematic axes, namely the "**Workshop on Quantum Key Distribution (QKD) Systems**" held on 18 and 19 of September and the the "Workshop on Cybersecurity with QKD Systems and Post-Quantum Cryptography (PQC)" held on 21 and 22 of September. The two workshops were well-received, with an average of 100 attendees at the first workshop and 75 at the second. In total, **175 unique people** attended the workshops. Additionally an average of **100 people per day participated online** via the GRNET Diavlos livestream service. **Sixteen trainers** provided insights and knowledge on quantum communication.

The new Secretary General of Telecommunications and Post, Konstantinos Karantzalos, addressed a welcome note to commence the 4-Day Training Event. The Secretary General mentioned: "I would like to recognize the previous leadership of the Ministry and GRNET for their work on this important project. I wish everyone a successful start to the 4-day training event".

The Chairman of the Board of Directors GRNET S.A., Prof. Stefanos Kollias, in his welcome speech stated: "Quantum technology is one of the technologies that already concern us and will be of great interest to us in the coming period. It will have an impact on all sectors. I am personally involved in machine learning and artificial intelligence and we're trying to develop technologies compatible with quantum technology. So we found ourselves today at an advanced meeting and training that concerns both engineers, researchers, and students. GRNET, as coordinator of the HellasQCI project, will strive in cooperation with

the partner universities to achieve the best education of engineers, students, and researchers in these technologies. I wish you a good start and good luck in this seminar".

The CNRS research director at Sorbonne University in Paris Dr. Eleni Diamanti was invited as a keynote speaker and presented the "Quantum Technologies - QKD Landscape in Europe". In her presentation she gave a generic overview of quantum technology and demonstrated the evolution of quantum technologies since the beginning of the 20th century. She showed the European Efforts in Quantum Communication in the period of 2016-2021 and she explained the EuroQCI goals toward the creation of an operational, integrated satellite and terrestrial system that covers the entire EU for the exchange of cryptographic keys in the highest level of security.

The HellasQCI Project Coordinator GRNET S.A., Dr Ilias Papastamatiou, in his presentation made an HellasQCI project overview and explained in detail the goals of HellasQCI and the aim of EuroQCI for the protection of sensitive data and the safety of the communication infrastructures.

The Aristotle University of Thessaloniki–AUTH Prof. Konstantinos Vyrsokinos, gave an Overview of Four Day HellasQCI Training.

The CNRS research director at Sorbonne University in Paris Dr. Eleni Diamanti presented the way communication is secured in a quantum world by showing the overall context of quantum communication networks and its combination with PQC (Post Quantum Cryptography) and the barriers that are overcomed with the use of quantum technology. She also presented the Paris Testbed deployment at the FranceQCI.

Principal Researcher of FORTH Dr Georgios Nikolopoulos analyzed the Basic Principles of Quantum Key Distribution and gave a brief introduction to QKD. He gave the related definitions of photons, and public key cryptography, he also showed the application of BB84 protocol in the communication process.

The Aristotle University of Thessaloniki–AUTH Prof. Konstantinos Vyrsokinos gave in his presentation an overview of the Quantum Ramdom Number Generators. He also explained that the QRNGs are base on quantum optics.

Assistant Professor at The National Kapodistrian University of Athens HellasQCI Technical coordinator George T. Kanellos divided his presentation in 3 sections, The first was an overview of status of QKD networks, the limitations of QKD technology, explained why a key management process is necessary and gave specific examples of QKD networks. In the second part investigated the emerging technologies that are essential for the deployment of the QKD networks such as Advanced QKD networks controls that are necessary to create large scale networks. In the final section provided specific definitions such as quantum entanglement, distribution, quantum teleportation, and how all that reflex to HellasQCI.

R&D Data Engineering from Space Hellas Mr Ilias Balabanis, gave an overview of encryption and decryption with QKDs and presented a proof of concept that was deployed within the EU OPENQKD project.

Post-doc Senior Researcher Giannis Giannoulis at the School of Electrical and Computer Engineering, Photonics Communications Research Laboratory of National Technical University of Athens in his presentation discussed about the building blocks that are used at the laboratory, what it is expected, what are the challenges and what can be handled at the laboratory when conducting single photon

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

experiments. He also provided the QKD System Architecture, he was focused on the Quantum Layer Implementation and Quantum Layer Evaluation.

Research Director from NCSR Demokritos – WP6 leader, Dr Homer Papadopoulos explained the evolvement of safe to quantum safe telecommunications. For the use case of Healthcare he analysed that QKD is not sufficient. He gave the definition of PQC and homomorphic encryption. Finally, he introduced the Healthcare use case being used in HellasQCI. He also gave a short overview of the forthcoming which was to set up an encryptor for a QKD Device.

Director of research in Walton Institute, Partner of the project, Dr Deidre Kilbane, presented the Quantum Communication Infrastructure for Ireland. She gave an overview of QKD National Network in Ireland and showed the use cases at the sectors of Banking & Finance, Cloud and Data Centre, Healthcare, Government and Defense.

Associate Professor at the Department of Electrical Engineering and Informatics of Cyprus University of Technology Dr Konstantinos Katzis presented the Cyprus Quantum Communication Infrastructure. In his presentation he briefly explained the architecture of QKD, the EuroQCI initiative and the objectives of CYQCI. He also explained the application of the QKD network in Cyprus and the use cases that are being developed. He also showed the establishment of the Optical Ground Station.

Coordinator of Polish Quantum Communication coming also from Poznan Supercomputing and Networking Center PSNC, Dr Piotr Rydlichowski presented what it is envisioned with the Polish QCI proposal how it relates to EuroQCI, as well as other projects connected with quantum communications and quantum technologies and how to develop secure communication scenarios and use cases.

The second day of the training event was hybrid as the first session was containing lectures at the central auditorium. The day lectures in terms of theory were about the space optics. The second session was containing experiments done in laboratory. The two laboratory sessions were conducted in the Photonics Communications Research Laboratory (PCRL) of NTUA and in the Optical Communications and Photonics Technology Laboratory at the National and Kapodistrian University of Athens.

Post doc researchers at the Photonics Communications Research Laboratory (PCRL) of NTUA Dr Nikolaos Lyras and Dr Argiris Ntanos presented QKD in Space, satellite ground QKD links. They showed the optical satellite communication systems, they continued to show the advances and the drawbacks of this technology, as well as the Challenges and opportunities. Lastly, they presented the technological steps that can be used in classical and space QKD communications systems and the benefits of space based QKDs.

Post doc researchers at the Photonics Communications Research Laboratory (PCRL) of NTUA Dr Aris Stathis, in his presentation he gave the theoretical background and described the equipment for the hands-on training. In his presentation he included the generation of photon pulses, the detection of photons, and explained the block of photons that were built in the laboratory.

The following session included the hands-on training that took place in NKUA and NTUA

In brief the NKUA at the optical Communications and Photonics Technology Laboratory National and Kapodistrian University of Athens, Department of Informatics and Telecommunications hands-on training included the basic set up of a QKD system and performed some tests over different meters of fiber.

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

The Laboratory session in the NTUA included the following

- Operating Principle of Single Photon Avalanche Detectors (SPAD)
- Coherent Light: Poissonian Photon statistics and single photon interference
- Generation, transmission and detection of encoded single-photons over a dark fiber
- Transmission and detection of single- photons over free space
- Coexistence of classical and quantum signals over converged fiber/FSO link

On the third day of the training event Senior Research Collaborator at ICS-FORTH, Dr Harry Manifavas presented the role of cryptography in cybersecurity, its weaknesses, adversarial settings, cryptography's weaknesses, security design criteria, and security strength levels.

In the next lesson **Dr Harry Manifavas** covered topics such as the fundamental cryptographic primitives, symmetric cryptography, public key cryptography, cryptographic hash functions, and their practical applications in real-life scenarios.

In the following **Dr Harry Manifavas,** discussed about various cryptographic attacks, including ciphertext-only and known-plaintext attacks, brute force attacks, cryptographic key length recommendations, public key algorithms security, factoring problems, man-in-the-middle and replay attacks, and cryptographic failures.

In the first session of the laboratory **Emmanouil Papadogiannakis from ICS FORTH** made demonstrations which involved attempting to attack a social network by bypassing authentication.

In the second session of the laboratory, he continued to show exploiting cryptographic failures, cipher misuse, and crypto misconfiguration.

On the fourth day of the training event **Dr Harry Manifavas** presented Post-quantum cryptography challenges in symmetric and public-key quantum computing, including retrospective decryption, Shor's and Grover's algorithms, threat mitigation, NIST PQC standardization effort, PQC transition recommendations, and cryptographic agility.

Afterwards, **Dr Harry Manifavas** introduced Quantum Cryptography and Quantum Encryption, discussing their use cases, requirements, security, and protocols, as well as their threats, limitations, and criticisms.

Research Director from NCSR Demokritos – WP6 leader, Dr Homer Papadopoulos explored the integration of Quantum Key Derivatives (QKD) into the cryptographic landscape, addressing challenges in practical deployment and exploring current trends in QKD standardization efforts.

In the following session **Collaborating Researcher at the eHealth & Knowledge Management Unit Mr Korakis Antonis and PhD Student for the University of Piraeus and an Early-Stage Researcher at NCSR Demokritos Mr Balaskas** George demonstrated how to extract QKD device keys, using PQC algorithms for digital signatures, encrypting files, and enabling computations on encrypted data without decryption.

Next in the practical session **Mr Antonis Korakis and George Balaskas** provided step-by-step instructions for setting up an encryptor and key retrieval from a QKD device, encrypting files with AES 256, using digital signatures, and understanding Homomorphic techniques for secure cloud computations.

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

Useful information about the HellasQCI project kick-off meeting and the project's objectives:

- DIAVLOS, GRNET's web streaming service recording or the high level welcome remarks: https://diavlos.grnet.gr/room/611?eventid=14792&vod=12369_event
- Meeting agenda and partners available here : https://hellasqci.eu/first-training-event/

Other useful links and info:

- HellasQCI info page on GRNET website: https://grnet.gr/business-directory/hellasqci/
- EuroQCI info website page
- HellasQCI portal (Home - HellasQCI)
- Official project Hashtag: #HellasQCI
- Official kick-off meeting Hashtag:
- GRNET Social Media Channels: Facebook, Twitter, LinkedIn, Instagram, YouTube

2. Training Event Photo material

Plenary Session at the Multimedia Amphitheater, NTUA, Athens

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

Prof. Konstantinos Karantzalos, Secretary General of Telecommunications & Posts, Hellenic Ministry of Digital Governance

Prof. Stefanos Kollias, Chairman of the Board of Directors GRNET S.A.

Keynote speech by Dr. Eleni Diamanti, CNRS research director at Sorbonne University, Paris

Prof. Konstantinos Vyrsokinos (AUTH), Prof. Stefanos Kollias (Chairman of the Board of Directors GRNET S.A.), Prof. Konstantinos Karantzalos (Secretary General of Telecommunications & Posts, Hellenic Ministry of Digital Governance), Dr. Ilias Papastamatiou, HellasQCI Project Coordinator, GRNET S.A., Ass. Prof. Kanellos (NKUA - HellasQCI Technical Coordinator), Yannis Rizopoulos, Journalist, Boussias Media

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

Dr. Homer Papadopoulos, (National Center for Scientific Research Demokritos), Dr. Johanna Sepúlveda Chief Engineer Quantum-Secure Communications, Airbus Defence and Space, Artemis Psarianou BA, DipM, ACIM, MA, AC, (Head of Marketing and Communications Department - GRNET S.A.), Prof. Konstantinos Vyrsokinos (AUTH), Dr. Ilias Papastamatiou, (HellasQCI Project Coordinator, GRNET S.A.), Yannis Rizopoulos, Journalist, (Boussias Media), Dr Deirdre Kilbane Director of Research in Walton Institute for Information and Communication Systems SETU, IrelandQCI Coordinator, Ass. Prof. Kanellos (NKUA - HellasQCI Technical Coordinator)

Photonics Communications Research Laboratory (PCRL) - Hands On Experience @ NTUA Operating Principle of Single Photon Avalanche Detectors (SPAD)

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

Research Laboratory - Hands On Experience @ NKUA National and Kapodistrian University of Athens

3. Training Event Media publications

https://tomanifesto.gr/hellasqci-theoritikes-kai-praktikes-gnoseis-sto-seminario-gia-tis-kvantikes-technologies-153848

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

4. Annex 1 – Full media publications (PDF)

NetFax #5134
Τρίτη
19|09|2023

Το μέλλον της κυβερνοασφάλειας είναι κβαντικό

Τετραήμερο εκπαιδευτικό σεμινάριο για το έργο HellasQCI

Σε μια εποχή που η καθημερινότητά μας εξαρτάται ολοένα περισσότερο από την ψηφιακή τεχνολογία, η κυβερνοασφάλεια αποτελεί καίριο παράγοντα, από τον οποίο ουσιαστικά εξαρτάται η ίδια η επιβίωσή μας. Οι κβαντικές τεχνολογίες -ώριμες πια και έτοιμες να ανταποδώσουν στην κοινωνία όσα έχουμε επενδύσει επάνω τους- θα αρχίσουν τα επόμενα χρόνια να δίνουν λύσεις σ' αυτό και πολλά άλλα θέματα, που ξεκινούν από τη μετεωρολογία και τους ταχύτατους υπολογιστές και φτάνουν ως την Τεχνητή Νοημοσύνη και τη Μηχανική Μάθηση. Όμως, πριν από την εφαρμογή, πρέπει βεβαίως να προηγηθούν η (θεωρητική και πρακτική) εκπαίδευση και εξοικείωση των χρηστών κι αυτός ακριβώς είναι ο στόχος του πρώτου τετραήμερου σεμιναρίου, στο πλαίσιο του ευρωπαϊκού συγχρηματοδοτούμενου έργου HellasQCI, που ξεκίνησε χθες, στις φιλόξενες εγκαταστάσεις του ΕΜΠ.
Το σεμινάριο, στο οποίο απηύθυνε χαιρετισμό ο νέος ΓΓ Τηλεπικοινωνιών και Ταχυδρομείων, Κωνσταντίνος Καράντζαλος υποσχόμενος τη στήριξη του, απευθύνεται στη νέα γενιά μηχανικών, επαγγελματίες της κυβερνοασφάλειας, αλλά και εκπροσώπους της πανεπιστημιακής κοινότητας, φοιτητές, ερευνητές και καθηγητές που εστιάζουν στους τομείς των οπτικών και κβαντικών τεχνολογιών, με απώτερο σκοπό την προετοιμασία της χώρας για τη λειτουργία της Ευρωπαϊκής Υποδομής Κβαντικών Επικοινωνιών EuroQCI, ειδικά σ' ό,τι αφορά στα κβαντικά «κλειδιά» και τη μετα-κβαντική κρυπτογραφία.

Εταίροι και συνέργειες

Εκτός από τους εταίρους του «HellasQCI» (Εθνικό Δίκτυο Υποδομών Τεχνολογίας και Έρευνας, Εθνικό Μετσόβιο Πολυτεχνείο, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών, Ίδρυμα Τεχνολογίας και Έρευνας, ΕΚΕΦΕ «Δημόκριτος», Αστεροσκοπείο Αθηνών και Space Hellas, στο σεμινάριο συμμετέχουν επίσης -αναδεικνύοντας τον διεθνή χαρακτήρα της ελληνικής προσπάθειας- απεσταλμένοι από τους διεθνείς εταίρους, τα αντίστοιχα Εθνικά Δίκτυα Κβαντικών Επικοινωνιών της Ιρλανδίας, της Πολωνίας, και της Κύπρου. Στην εναρκτήρια συνεδρίαση του σεμιναρίου και μετά τον χαιρετισμό του προέδρου του ΕΔΥΤΕ, καθ. Στέφανου Κόλλια, η κύρια ομιλήτρια, Δρ. Ελένη Διαμαντή (διευθ. ερευνών του CNRS, στη Σορβόννη), έδωσε τη διεθνή εικόνα των δυνατοτήτων των κβαντικών τεχνολογιών και των εφαρμογών τους με συγκεκριμένα παραδείγματα από τη Χημεία, τη Φαρμακολογία, τις Χρηματοοικονομικές υπηρεσίες , τα νέα Υλικά, την Ιατρική, τη Μετρολογία, την Άμυνα, και, φυσικά, την ασφάλεια, ειδικά των κρίσιμων υποδομών, τονίζοντας ότι μπορούμε να καταφέρουμε πολλά.. Την ελληνική πραγματικότητα (ενταγμένη, προφανώς, στην ευρωπαϊκή εικόνα, όπου οι προτάσεις μας διακρίνονται ιδιαίτερα - πέρυσι, αναδείχθηκαν δεύτερες καλύτερες στην ΕΕ) περιέγραψε το στέλεχος του ΕΔΥΤΕ και συντονιστής του HellasQCI, Δρ. Ηλίας Παπασταμάτιου. Ανέλυσε τη δομή του επίγειου (ετοιμάζονται 12 κόμβοι ανά την Ελλάδα) και του δορυφορικού σκέλους (γίνονται εργασίες στα αστεροσκοπεία του Χελμού, του Χολομώντα και του Σκίνακα, για την υποδοχή των κβαντικών σημάτων και τη σύνδεση με τα κοντινά μητροπολιτικά κέντρα) και αποκάλυψε πως ο χρονικός στόχος για τη λειτουργία του συστήματος, είναι το 2027.

ΓΙΑΝΝΗΣ ΡΙΖΟΠΟΥΛΟΣ

LANCOM: ΑΝΑΔΕΙΞΗ ΤΗΣ ΧΩΡΑΣ ΣΕ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΟ ΚΟΜΒΟ ΤΩΝ ΒΑΛΚΑΝΙΩΝ

Στο Βελιγράδι και στην Πράγα παρευρέθηκαν για άλλη μία χρονιά τα στελέχη της Lancom συμμετέχοντας στο Central and Eastern Europe Carriers and Enterprises Event και στο European Peering Forum αντίστοιχα.
Το CEE CEE Summer Event 2023, που πραγματοποιήθηκε στις 7-8 Σεπτεμβρίου, συγκέντρωσε τα κορυφαία στελέχη του κλάδου των τηλεπικοινωνιών της Κεντροανατολικής Ευρώπης σε στοχευμένες επιχειρηματικές συναντήσεις. Ακολούθως, στις 11- 13 Σεπτεμβρίου στην Πράγα, στο European Peering Forum, μια εκδήλωση έντονου ενδιαφέροντος για τηλεπικοινωνιακούς παρόχους και εκπροσώπους Internet Exchanges, τα στελέχη της Lancom πραγματοποίησαν εκτός των τεχνικών σεμιναρίων και πλήθος συνομιλιών με υπάρχοντες και εν δυνάμει συνεργάτες.

Παραγωγικές συναντήσεις

Κατά τη διάρκεια των δύο συνεδρίων, τα στελέχη της Lancom παρουσίασαν το όραμα της εταιρείας για την ανάδειξη της χώρας στο νέο τηλεπικοινωνιακό κόμβο των Βαλκανίων, με όχημα το Balkan Gate Thessaloniki, το οποίο, όπως αναφέρεται, «πλέον χαίρει διεθνούς αναγνώρισης καθώς έχει συγκεντρώσει και παρέχει υπηρεσίες φιλοξενίας-διασύνδεσης σε μερικές από τις μεγαλύτερες πολυεθνικές και ελληνικές εταιρείες τηλεπικοινωνιών». «Οι συναντήσεις μας στο εξωτερικό ήταν ιδιαίτερα παραγωγικές, και περιμένουμε να ανακοινώσουμε πολλές νέες σημαντικές συνεργασίες μέσα στους επόμενους μήνες», δήλωσε η διευθύντρια πωλήσεων της Lancom Λένα Ξανθοπούλου.

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

5. Annex 2 – Kick-off agenda

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

HellasQCI - Quantum Communication Infrastructure for Greece

HellasQCI
Four-Day Training Event

18-19 & 21-22 September 2023

National Technical University of Athens

Zografou campus

Co-funded by the European Union

EuroQCI

Co-funded by the European Union

The HellasQCI Project has received funding under the Grant Agreement No. 101091504

HellasQCI - Quantum Communication Infrastructure for Greece

Program of the Workshop on Quantum Key Distribution (QKD) Systems

1st Day Training - September 18th, 2023

Welcoming Session

(In this session spoken Language will be Greek)

Moderator: Yannis Rizopoulos, Journalist, Boussias Media

Location: NTUA Zografou Campus Multimedia Amphitheatre on the basement of the NTUA Central Library

Directions: https://goo.gl/maps/NkcFx7woMTUMNc2q9

08:30-09:00	Registration
09:00 – 09:10	Welcoming Remarks by Prof. Konstantinos Karantzalos, Secretary General of Telecommunications & Posts, Hellenic Ministry of Digital Governance
09:10 – 09:20	Welcoming Remarks by Prof. Stefanos Kollias, Chairman of the Board of Directors GRNET S.A.
09:20 – 09:25	Welcoming Remarks by the European Commission (video message)
09:25 – 09:40	Keynote speech "Quantum Technologies - QKD Landscape in Europe" by Dr. Eleni Diamanti, CNRS research director at Sorbonne University in Paris
09:40 – 09:50	"HellasQCI project overview and synergies with EuroQCI" by Dr. Ilias Papastamatiou, HellasQCI Project Coordinator, GRNET S.A.

Co-funded by the European Union

EuroQCI

HellasQCI - Quantum Communication Infrastructure for Greece

09:50 – 09:55	"Overview of Four Day HellasQCI Training" by Prof. Konstantinos Vyrsokinos, Aristotle University of Thessaloniki - AUTH
09:55 – 10:10	**Q&A**
10:10 – 10:25	**Coffee Break**

Second Session:

(Spoken Language will be English)

Moderator: Yiannis Yianoulis, NTUA

Location: NTUA Zografou Campus Multimedia Amphitheatre on the basement of the NTUA Central Library

Directions: https://goo.gl/maps/NkcFx7woMTUMNc2q9

10:25 – 11:00	Eleni Diamanti, CNRS CNRS research director at Sorbonne University in Paris Plenary Session
11:00 – 11:30	George Nikolopoulos, FORTH Basic Principles of QKD
11:30 – 12:15	Konstantinos Vyrsokinos, AUTH QRNGs
12:15 – 13:00	George Kanellos, NKUA QKD Networks
13:00 – 14:00	**Lunch Break**
14:00 – 14:45	Giannis Giannoulis, NTUA/GRNET From billion photons to single photon experimental setups

Co-funded by the European Union

EuroQCI

14:45 – 15:05	Ilias Balampanis, Space Hellas SA QKD with Raspberry PI's as encryptors/decryptors
15:05 – 15:30	Homer Papadopoulos, NCSRD QKD with PQC for a Healthcare use case
15:30 – 15:45	Deirdre Kilbane, WIT IrelandQCI
15:45 – 16:00	Konstantinos Katzis, EUC CyQCI
16:00 – 16:15	Piotr Rydlichowski, PSNC PIONIER- Q
16:15-16:45	Conclusions and Discussion (Q&A)

2nd Day Training - September 19th, 2023

(Spoken Language will be English)

Moderator: Konstantinos Vyrsokinos, AUTH

Location: NTUA Zografou Campus, Multimedia Amphitheatre on the basement of the NTUA Central Library

Directions: https://goo.gl/maps/NkcFx7woMTUMNc2q9

09:00 – 10:00	Aris Stathis, Argiris Ntanos, NTUA/GRNET Theoretical background and equipment description for hands-on experiments
10:00 – 10:45	Nikos Lyras, Argiris Ntanos, NTUA/GRNET QKD in Space, satellite-to-ground QKD links
10:45 -11:00	**Coffee Break**
Change Room: Photonics Communications Research Laboratory (PCRL) **Directions: https://goo.gl/maps/4CyFnLFENcgkX3GN9**	

Co-funded by the European Union EuroQCI

HellasQCI - Quantum Communication Infrastructure for Greece

11:00 -13:00	Hands On Experience @ NTUA Operating Principle of Single Photon Avalanche Detectors (SPAD) Coherent Light: Poissonian Photon statistics and single photon interference Generation, transmission and detection of encoded single-photons over a dark fiber Transmission and detection of single- photons over free space Coexistence of classical and quantum signals over converged fiber/FSO link
13:00 – 14:00	**Lunch Break**
14:00 – 17:00	Hands-On Experience @ NKUA Optical Communications and Photonics Technology Laboratory (Room Y2) National and Kapodistrian University of Athens Department of Informatics and Telecommunications Panepistimiopolis, Ilisia Athens, 16122 https://www.di.uoa.gr/department/contact-location

Co-funded by the European Union

EuroQCI

HellasQCI - Quantum Communication Infrastructure for Greece

Program of the Workshop on Cybersecurity with QKD Systems and Post-Quantum Cryptography (PQC)

3rd Day Training - September 21st, 2023: Introduction to cryptography
Lectures and hands on experience

(Spoken Language will be English)

Moderator: Harry Manifavas, FORTH

Location: NTUA Zografou Campus Multimedia Amphitheatre on the basement of the NTUA Central Library

Directions: https://goo.gl/maps/NkcFx7woMTUMNc2q9

09:00 - 09:15	Welcome Session
09:15 – 10:15	Harry Manifavas, FORTH Cybersecurity and the role of Cryptography The Weakest Link Property The Adversarial Setting Cryptography Pitfalls Security and Other Design Criteria Security Strength levels
10:15 - 11:00	Harry Manifavas, FORTH Basic cryptographic primitives Symmetric Cryptography Public Key Cryptography Cryptographic Hash Functions Applications of cryptography in real life
11:00 – 11:15	Coffee Break
11:15 – 12:00	Harry Manifavas, FORTH

Co-funded by the European Union

EuroQCI

	Cryptographic Attacks and Failures Ciphertext-Only and Known-Plaintext Attacks Brute Force Attack Cryptographic key length Recommendations Public Key Algorithms Security The Factoring Problem Man-in-The-Middle and Replay Attacks Cryptographic Failures: Case Studies
12:00 - 13:00	Emmanouil Papadogiannakis, FORTH Demonstrations Attacking a social network Bypassing authentication
13:00- 14:00	Lunch Break
14:00 – 17:00	Emmanouil Papadogiannakis, FORTH Practice session: labs and exercises Exploiting cryptographic failures Cipher misuse Crypto misconfiguration

4th Day Training - September 22nd, 2023: Introduction to Post Quantum Cryptography and Quantum Key Distribution

Lectures and hands on experience

(Spoken Language will be English)

Moderator: Homer Papadopoulos, NCSRD

Location: NTUA Zografou Campus Multimedia Amphitheatre on the basement of the NTUA Central Library

Directions: https://goo.gl/maps/NkcFx7woMTUMNc2q9

09:00 – 10:00	Harry Manifavas, FORTH Introduction to Post-Quantum Cryptography Quantum Computing Threat Landscape for Symmetric and Public-Key Cryptography Challenges: Retrospective Decryption, Shor's and Grover's Algorithms Quantum Computing Threat Mitigation Post-quantum Cryptography NIST PQC Standardization Effort PQC Transition Recommendations and Cryptographic Agility
10:00 – 11:00	Harry Manifavas, FORTH Introduction to QKD Quantum Cryptography and Quantum Encryption QKD Use Cases QKD Requirements, Security and Protocols Attacks and Limitations Challenges and Criticism Quantum Random Number Generators
11:00 – 11:15	*Coffee Break*

Co-funded by the European Union

EuroQCI

HellasQCI - Quantum Communication Infrastructure for Greece

11:15 – 12:00	Homer Papadopoulos, NCSRD Integrating QKD into the existing Cryptographic Landscape: Addressing Challenges in Practical Deployments of QKD and Quantum-Safe Cryptography, and Exploring Current Trends QKD standardization efforts and challenges EuroQCI
12:00 - 13:00	Antonis Korakis, George Balaskas, Homer Papadopoulos NCSRD Demonstrations Extract keys from a QKD device. Digital signatures with PQC algorithms Encrypt files with PQC algorithms Enable computations on encrypted data without decryption.
13:00- 14:00	*Lunch Break*
14:00 – 17:00	Antonis Korakis, George Balaskas, Homer Papadopoulos NCSRD Practice session: labs and exercises Walk through step-by-step instructions for setting up the encryptor and key retrieval from the QKD device. Encrypt your files with AES 256. Set up your own digital signatures using PQC Dilithium library to authenticate yourself to the encryptor. Encrypt your files with PQC Kyber's encryption methods to access the encryptor.

Co-funded by the European Union

EuroQCI

	Learn the Homomorphic techniques for encrypting your files, enabling secure cloud computations, while maintaining complete data encryption