CELTIC-NEXT
Proposers Brokerage Day
30th January 2026, Vienna

Q-TRUST6G
Quantum-Resilient Trust Framework for Secure 6G Systems

Dr. Faruk SARI
faruk.sari@cyber-quanta.com

Teaser

Towards trustworthy 6G systems by combining PQC-based identity trust with channel-based secret key generation for frequent symmetric rekeying.

Main Benefit

- *Strengthens identity trust, authenticity and session-level confidentiality in future 6G networks.*
- *Addresses quantum-era threats and real-time radio-layer attacks together*
- *Enables secure operation of IoT and cyber-physical systems*

Added Value

- *Hybrid approach combining:*
  - Post-Quantum Cryptography (PQC)
  - Physical Layer Security (PLS)
- *Goes beyond classical cryptography by adding continuous physical authenticity*
- *PLS is addressed via channel-based secret key generation (SKG/CBKG) to derive short-lived symmetric session keys.*
- *Applicable to realistic 6G use cases*

Why participate?

- *Shape future 6G security architectures*
- *Strong academic–industrial collaboration potential*
- *High relevance for telecom, IoT, CPS and critical communications*

Q-TRUST6G, Dr. Faruk SARI, Cyber Quanta, faruk.sari@cyber-quanta.com

Organisation Profile

Cyber Quanta (CQ) is a cybersecurity technology company focusing on:

- Post-Quantum Cryptography (PQC)
- PKI, certificate and key management
- Secure communications and IoT security
- Quantum-safe migration strategies

CQ develops advanced security architectures for critical infrastructures and next-generation communication systems, with strong expertise in cryptographic trust and key management.

•Based in **Teknopark İstanbul**, Türkiye

Proposal Introduction (1)

Vision & Motivation

6G networks will interconnect massive cyber-physical systems under strict latency, reliability and security requirements. At the same time, quantum computing threatens the long-term security of today's public-key cryptography.

Project Idea

A hybrid security framework that:

- Establishes long-term device identity trust using PQC
- Derives short-lived symmetric session keys via channel-based SKG/CBKG for traffic protection

This project advances hybrid PQC and PLS from concept level towards realistic testbed validation for 6G systems.

Proposal Introduction (2)

Expected Outcomes

- Validated hybrid PQC + SKG/CBKG-based physical-layer security framework for 6G environments
- Integrated prototype(s) demonstrated in representative wireless testbeds
- System architecture, interfaces and implementation guidelines aligned for future deployment
- Pathway to industrial adoption and standardization (to be refined with partners)

Expected Impact

- Quantum-resilient wireless security enablers for future 6G systems
- Enhanced protection against impersonation, spoofing and physical-layer attacks
- Aiming to reduce security overhead by enabling frequent SKG-based session rekeying
- High relevance for critical infrastructure, IoT and industrial communications (6G CPS)

Schedule (36 Months)

- 0–12: System design & integration
- 13–24: Prototype development & lab validation
- 25–36: Testbed validation & pilot demonstrations

Partners

Consortium Members

- Cyber Quanta (Türkiye-SME): System integration, PQC-based identity trust, key management & orchestration, secure communications
- ULAK Haberleşme (Türkiye-IND):
- MEDIPOL University (Türkiye-ACAD):
- TU Dortmund University (Germany-ACAD):
- Open Radio Systems (Germany-SME):
- PHYSEC GmbH (Germany-SME):
- Linköping University, (Sweden-ACAD):
- Brno University of Technology (Czech-ACAD):

Looking For Partners With Expertise In:

- We are looking for dedicated SMEs working on 6G security, together with partners experienced in channel-based key generation and real network validation
- Dedicated SME (EU): Active R&D on 6G Security and secure wireless systems
- SME / Academia: Expertise in Channel-Based Key Generation (CKG) and physical-layer key agreement
- Industry / Research Labs: 6G laboratory and testbed capabilities and Advanced simulation and emulation infrastructures
- Network Operator: Real network integration and field validation in operational environments

Contact Info

For more information and for interest to participate please contact:

Dr. Faruk SARI, Cyber Quanta

faruk.sari@cyber-quanta.com

+90 216 212 55 40

Teknopark Istanbul, NO: 1 /4C-213- Pendik/ ISTANBUL

www.cyber-quanta.com

Presentation is available via:

Join the Consortium Building Sessions

4. February
from 14:00-15:00 CET

Connection details:
Via
www.celticnext.eu/new-ideas