



SECURING TOMORROW'S DIGITAL INFRASTRUCTURE WITH QUANTUM-RESISTANT CRYPTOGRAPHY

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

PROJECT FACTSHEET

CATEGORY	DETAILS
PROJECT NAME	Q-FENCE: Securing Tomorrow's Digital Infrastructure with Quantum-Resistant Cryptography
GRANT AGREEMENT	N° 101225708
FUNDING PROGRAM	European Union's Horizon Europe & Swiss State Secretariat for Education, Research and Innovation (SERI)
COORDINATOR	South East Technological University (SETU), Ireland
SCIENTIFIC LEAD	Institute of Theoretical and Applied Informatics (IITIS), Poland
CONSORTIUM	15 partners from across Europe
LEAD CONTACT	Dr. Indrakshi Dey

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**



Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

OUR MOTIVATION

- **Quantum threat:** Up to 31% probability that quantum computers could break current encryption by 2030
- **“Store now, decrypt later”:** Data collected today may be decrypted in the future



- **Economic impact:** Data breaches cost ~€4.5M on average, with high risks for critical sectors
- **Transition challenge:** Moving to post-quantum cryptography is complex—Q-FENCE enables a phased, hybrid approach

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

OUR MISSION

Q-FENCE is developing a pioneering dual-layer cryptographic framework to safeguard critical European sectors against the emerging threats of the quantum era.



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

THE DUAL FRAMEWORK

Two layers. One future-proof defense.



Advanced encryption (soft-core): Uses cutting-edge methods like Ring-LWE and Module-LWE, enhanced with Quantum Random Number Generation (QRNG), to create highly secure and unpredictable encryption keys.



Hardware Root-of-Trust Core: Built-in hardware security (hard-core): Leverages unique chip “fingerprints”, Physically Unclonable Functions (PUFs), to ensure secure device identity, trusted start-up, and protection against tampering.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

OBJECTIVES

ADVANCE PQC MATURITY

Develop a robust dual-layer framework and establish rigorous risk-based performance metrics.

SECURE HYBRID TRANSITION

Integrate existing algorithms (like RSA) with new quantum-resistant protocols for a gradual transition.

PHASED DEPLOYMENT

Design modular cryptographic components tailored for specific sectors to avoid operational disruption.

SECTOR-SPECIFIC VALIDATION

Deploy demonstrators on varied platforms like IoT, satellite systems, and cloud networks.

EU-WIDE RECOMMENDATIONS

Generate application-oriented guidelines focused on compliance with GDPR and the NIS2 directive.

AWARENESS & CULTURE

Foster a common cybersecurity culture through educational campaigns and workshops for policymakers and the public.

COMMERCIAL EXPLOITATION

Define a clear strategy for IP protection and a business roadmap for marketable solutions.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE



PROJECT OUTCOMES



MATURE & STANDARDIZED ALGORITHMS

Advances cryptographic maturity to meet rigorous security standards and support global standardization.



PHASED DEPLOYMENT

Enables the gradual phase-in of quantum-safe protocols into existing applications to ensure compatibility.



USER-FRIENDLY IMPLEMENTATION TOOLS

Creates accessible, modular tools for seamless integration into diverse platforms like IoT and cloud systems.



VALIDATED DEMONSTRATORS

Proves framework adaptability and efficiency across diverse hardware in real-world conditions.



SECURE HYBRID TRANSITION

Combines classical and post-quantum protocols for a phased transition without disrupting legacy operations.



EU-WIDE RECOMMENDATIONS

Generates GDPR-aligned guidelines to help organizations reduce deployment time and costs.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



Funded by
the European Union



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Project funded by

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE



FINANCE

HEALTHCARE

SMART CITIES

SATELLITE
NETWORKS

ENTERPRISE
NETWORKS

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

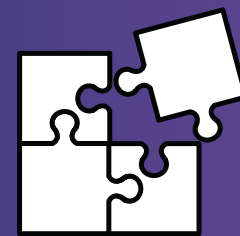
Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

FINANCE

CROSS-BANK ANTI-MONEY LAUNDERING (AML)



THE CHALLENGE

Financial institutions must detect irregular patterns across different banks, but privacy laws prevent sharing raw customer data.



THE SOLUTION

A cross-bank system using Secure Multi-Party Computation (MPC) and Homomorphic Encryption (HE) to analyze data without revealing private details.



KEY FEATURE

Computing Risk Scores in an encrypted layer, never revealing raw client data, only risk bands. Auditing aided by a tamper-proof logbook secured by post-quantum signatures.



LOCATION

Luxembourg (University of Luxembourg)

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

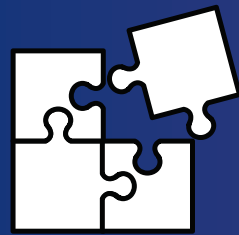
Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

HEALTHCARE

SECURE HEALTH DATA SHARING



THE CHALLENGE

Sharing medical data is high-risk and vulnerable to "harvest now, decrypt later" attacks due to the long lifetime of health records.



THE SOLUTION

A hybrid base station combining classical and quantum resources with Homomorphic Encryption (HE) to process data without decryption.



KEY FEATURE

Ensures data integrity, secure patient authentication, and full compliance with GDPR.



LOCATION

Silesia region, Poland (Institute of Applied and Theoretical Informatics, IITiS)



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**



Project funded by

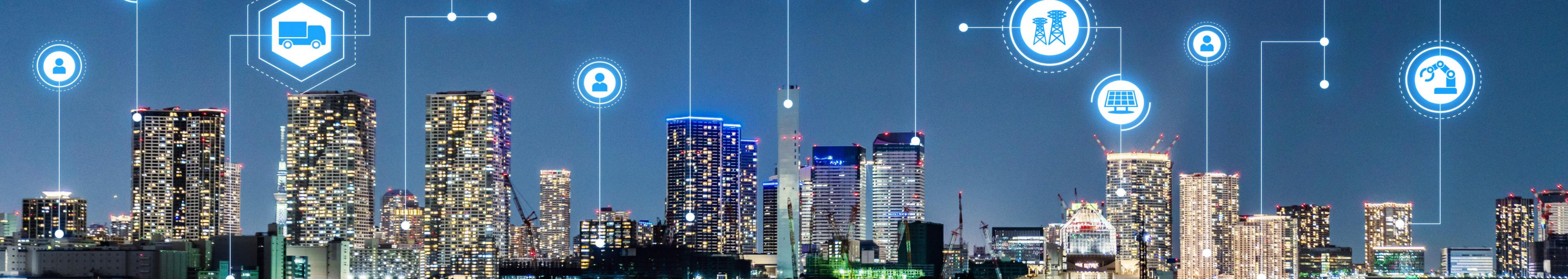
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

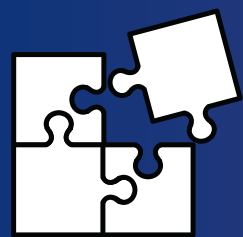


Q-FENCE



SMART CITIES

SECURING IOT DATA AGGREGATION



THE CHALLENGE

Massive networks of IoT sensors are vulnerable to cloning and hacking, often operating with limited power and security.



THE SOLUTION

Combining Physically Unclonable Functions (PUFs) and Quantum Random Number Generators (QRNGs) to create unique, unclonable device identities.



KEY FEATURE

PQ secure boot and Feedback Vertex Set (FVS) optimization to streamline data flow and reduce network congestion.



LOCATION

Geneva, Switzerland (IoT Lab Virtual Testbed)

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

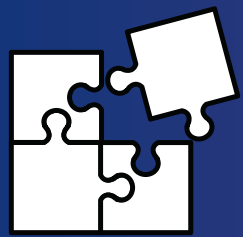
Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

SATELLITE NETWORKS

QUANTUM-SAFE SPACE COMMUNICATION



THE CHALLENGE

High-latency satellite-ground links are vulnerable to interception and future quantum-enabled cyberattacks.



THE SOLUTION

A framework securing links with hardware-based roots of trust (PUFs/QRNGs) and Homomorphic Encryption for telemetry data.



KEY FEATURE

Mermin-Peres Magic Square Game (quantum game theory) to detect eavesdropping on communication channels.



LOCATION

Fucino Telespazio Space Center and the Rome Telespazio Headquarters, Italy



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

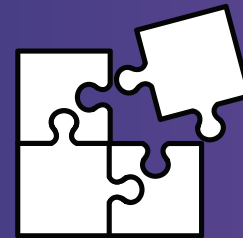
Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

ENTREPRISE NETWORKS

BIDIRECTIONAL QUANTUM-RESISTANT CONNECTION



THE CHALLENGE

Large enterprises need massive transfer speeds between data centers, making fiber connections prime targets for interception.



THE SOLUTION

Integrating Quantum Key Distribution (QKD) with the Q-FENCE cryptographic core to provide defense-in-depth.



KEY FEATURE

Testing and benchmarking QKD-enhanced security on real-world fiber infrastructure between major cities.



LOCATION

Fiber network between Waterford, Cork, and Dublin, Ireland.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

Q-FENCE PARTNERS



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



Funded by
the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



Q-FENCE

THANK YOU !

GET IN TOUCH WITH US



@Q-FENCE

www.qfence-project.eu

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).



Funded by
the European Union

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI