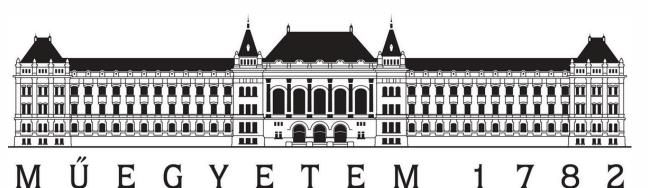
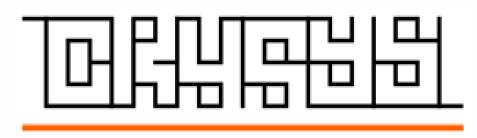
SECURING EUROPE'S DIGITAL FUTURE: FROM CYBER RESILENCE TO POST-QUANTUM CRYPTOGRAPHY







CrySyS Lab



Budapest University of Technology and Economics www.crysys.hu

Who we are

- CrySyS Lab:
 - Laboratory of Cryptography and System Security
 - o partner in 8 successful EU projects
 - research areas include:
 - Security of embedded systems
 - ML security
 - Malware detection
 - Applied Cryptography
- Me:
 - Post-doc at Uni. Wuppertal, Germany
 - CrySyS Lab alumni, return in 2026-Q2

What we do

Recent work on PQ Crypto:

- AAECC'23: proposed PQ
 - Verifiable Random Function
 - Oblivious Pseudorandom **F**unction
- *CRYPTO'23*: analysed WhatsApp's non-PQ solution for Password Protected Key Retrieval (PPKR)
- *CCS'24*: proposed PQ-secure **PPKR**

What we are looking for

A forming consortium, interested in

- PQ-PETS
- PQ-Transition
- Hybrid schemes
- Provably secure solutions
- Adopting PQ solutions to resource constrained environments

Máté Horváth **Contact details:** mhorvath@crysys.hu







Eötvös Loránd University, Faculty of Informatics (Péter Kutas, kuppabt@inf.elte.hu)

Who we are:

- Strong research track record
- Partnerships with several strong European univeristies (e.g., KU Leuven and TU Graz)
- Funding from EU and Hungarian grants

What we do:

- Post-quantum cryptography and computational number theory
- Applied cryptography and side-channel analysis
- Background in organizing large-scale events

What we are looking for:

- Industry partners with realworld applications
- Academic partners with an expertise in quantum computing

Slovenia SME focused on 360° Cyber Resilience, Cryptography, and AI-Powered Solutions

Who we are

- ESA project (PQC KEM related)
- PQ-REACT project (PQC signatures in smart meters)
- part of 3 CAT-B projects with EDA
- Horizon 2024

What we do

- implementation of PQC algorithms into wider applications
- optimising and testing various PQC migration scenarios

What we are looking for

Joining an HE consortium focusing on PQC migration with well defined, real-world usecases

Contact details

Matjaž Breznik, matjaz.breznik@creaplus.com



Slovak University of Technology in Bratislava Faculty of Electrical Engineering and Information Technology

Who we are

- A research group featuring 2 professors (<u>Pavol Zajac</u>, <u>Otokar</u> Grošek)
- Experience from 3 NATO
 SPS projects focused on
 PQC (Most recent
 project: link)

What we do

- Security analysis of PQC algorithms, including sidechannel attacks (Example paper: <u>link</u>)
- Implementation of quantum-resistant software (Example paper: <u>link</u>)

What we are looking for

Joining a consortium working towards submitting a HE project in 2025 in one of the following areas:

- Security analysis of PQC algorithms
- Secure implementation of PQC algorithms
- Integration of PQC algorithms into higher-level protocols
- Privacy enhancing technologies employing PQC algorithms

Contact details: <u>Tomas Fabsic</u>, email: tomas.fabsic@stuba.sk

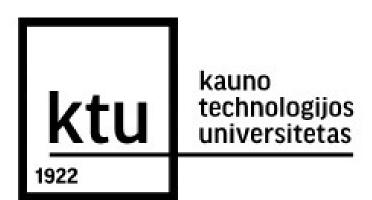
Matrix Power Function (MPF) based post-quantum cryptography

MPF is a matrix powered by the other two matrices from the left and the right hence obtaining the other matrix

TherearesomeevidencesthatMPF problem is NP-complete and therefore it can be used to create post-quantum cryptographic methods

Our activity:

Creation of new methods for KAP, Encryption, Identification, E-signature, etc. Perspective application of MPF based cryptography in blockchain technology. We need a partners for cooperation.



Prof. dr. Eligijus Sakalauskas,
Kaunas University of Technology,
Department of Applied Mathematics,

Chief of Research group: "Cryptography and blockchain systems".

Eligijus.Sakalauskas@ktu.lt







Who we are

- IT Security consulting for large & medium sized critical infrastucture providers
- in DACH region (**Softline**) and Baltics (**Squalio**) as part of global **NoventIQ** group

What we do

- Cryptographic Inventories
- PQC migration planning
- Cryptographic Key
 Management

What we are looking for

- join research consortia as industry partner for
 - CryptographicInventorization
 - PQC migration
- deliver valuable knowledge
 from real-world IT
 infrastructure (constraints)
 using classical cryptography

Contact details

Florian Schröck - <u>florian.schroeck@softline.de</u> or <u>LinkedIn</u>



Who we are

What we do

What we are looking for

The Baltic Institute of Advanced Technology (BPTI) is a private, high tech-oriented research institute.

We are driven by our mission to create value by providing R&D services for global security.

Al Research Group:

OT Sensor Technology

Automated Risk and Vulnerability
Assessment

Drone Pentesting

Partnerships for PQC applications for defense (EDF, etc.)

Opportunities to pilot our software

R&D opportunities and collaboration

Business partnerships

Contact details

www.bpti.eu

monika.venckauskaite@bpti.eu



Who we are

A Maltese quantum-secured communication startup

Significant experience with EU projects (Horizon Europe & Digital Europe), NATO SPS

Experienced in deploying complex quantum networks

What we do

We design quantum-secure networks **for the real world**

We **bridge the gap** between quantum communication technologies and end users

We speak both quantum and post-quantum cryptography

What we are looking for

Projects to join that include a quantum or post-quantum cryptography component

Organisations that wish to set up **proofs-of-concept** for quantum key distribution

Anything interesting!

Contact details

André Xuereb (Founder & CEO) – andre@merqury.eu





DevSlate Group, UAB

Who we are

DevSlate Group end-to-end software development, cybersecurity, and blockchain solutions.

BCCS Cluster
 digital innovation hub
 fostering fintech and
 Web3 industry growth.

What we do

- Cybersecurity &
 Compliance
- Custom Software Development
- Blockchain & Web3
 Solutions
- Networking & Knowledge Sharing

What we are looking for

Joining and forming HE and other EU program consortiums focusing on:

- Cybersecurity & Data Protection
- Digital Innovation & Emerging Technologies

Contact details

Vytenis Kazanavicius, COO Email: vytenis.kazanavicius@bccs.tech



Perlab

Telematic Engineering Department Universidad Carlos III de Madrid



Who we are

The Pervasive Computing Laboratory (**Perlab**) consists of 12 professors, researchers and students doing research across cybersecurity domains including:

- Post-Quantum Cryptography
- Internet of Things security
- Authentication methods
- Anomaly detection & intrusion prevention
- Privacy protection technologies
- Machine learning for security applications
- Network protocol analysis

What we do

Our PQC expertise:

- Integration of PQC into IoT protocols (CoAP, MQTT-SN, DDS, Zenoh) and robotics applications (ROS 2)
- Hybrid PQC + QKD integrations (IPSec, TLS, ETSI 004, ETSI 014)
- Hardware implementations (FPGA) and sidechannel attack mitigations
- Quantum cryptanalysis for lattice cryptosystems
- Experience in national projects like: QURSA:
 QUantum-based Resistant Architectures and
 Techniques (Spanish funded)
- We also led a HORIZON-CL3-2024-CS-01-02 proposal: QUASAR: Quantum-Agile Security for Automation and Robotics

What we are looking for

We are seeking partners for proposals in:

- Applied Post-Quantum Cryptography
 - Extending our work on protocol integration and optimization
 - Hardware-based security solutions with PQC readiness
 - Side-channel attack resistance in PQC implementations
- Quantum Cryptanalysis
 - Physics-based approaches to cryptanalysis
 - Hardness evaluation of lattice-based cryptosystems
- Privacy-Preserving Technologies
 - Privacy-enhancing mechanisms in network protocols (e.g., DNS)
 - Post-quantum secure PETs

Contact details: Javier Blanco-Romero (PhD Student) frblanco@pa.uc3m.es



