Participating Institutions

Slovak University of Technology (STU)

The Faculty of Electrical Engineering and Information Technology of STU is one of the oldest technical faculties in Slovakia with rich scientific and research activities. It has the mission to offer quality academic education to all degrees on the basis of free scientific research and creative experimental development. In addition, its academic community affiliates the transmission of scientific results into practice.

University of Malta (UoM)

UoM is the highest teaching institution in Malta catering for some 11,500 students from 92 different countries. Researchers at UoM conduct research in a variety of areas ranging from adaptive systems to seismic monitoring. The university is also home to a number of leading research programmes, including digital games research, climate change, metamaterials, physical oceanography and maritime law.

The University of Alabama in Huntsville (UAH)

UAH is a public research university serving close to 10,000 students. The National Security Agency and the Department of Homeland Security designated UAH a National Center of Academic Excellence in Cyber Defense (CAE-CD) and Research (CAE-R).

Universidad Rey Juan Carlos (URJC)

Founded in 1996, URJC is today the second largest public university of the Madrid region serving over 40,000 students. The University has focused its teaching and interdisciplinary research to find solutions to current industrial problems, and ranks among the best universities in Madrid for excellence academic programs and international scientific quality.

This Multi-Year Project is supported by the **NATO Science for Peace and Security (SPS) Programme.**

The SPS Programme develops and implements practical cooperation and enhances dialogue between NATO nations and Partner countries through capacity-building and security-related civil science, technology and innovation. All Programme activities contribute towards the Alliance's strategic objectives, have a clear link to security and respond to at least one of the SPS Key Priorities.

You can find further information on our website

www.nato.int/science

@NATO_SPS

sps.info@hq.nato.int

0778-21 NATO Graphics & Printing

The Emerging Security Challenges Division

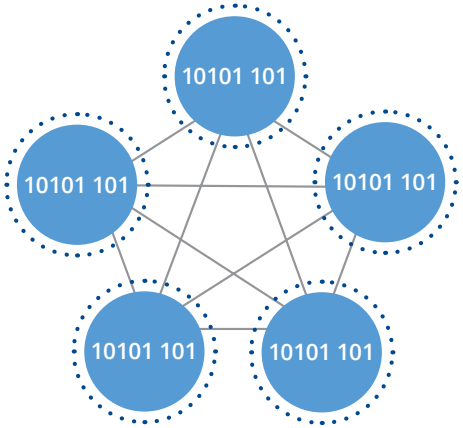
SECURE COMMUNICATION IN THE QUANTUM ERA

THE NATO
SCIENCE FOR PEACE AND SECURITY
SPS PROGRAMME

Goals

Reliable cryptographic solutions to protect the evolving information technology infrastructure remain vital. With quantum computing on the horizon, new solutions are needed, as key security features that are part of many existing cryptographic solutions will be broken once large-scale quantum computing capabilities will become widely available.

The goal of this SPS research project is to provide quantum-safe solutions for fundamental cryptographic algorithms, which are currently the base for securing digital communications.



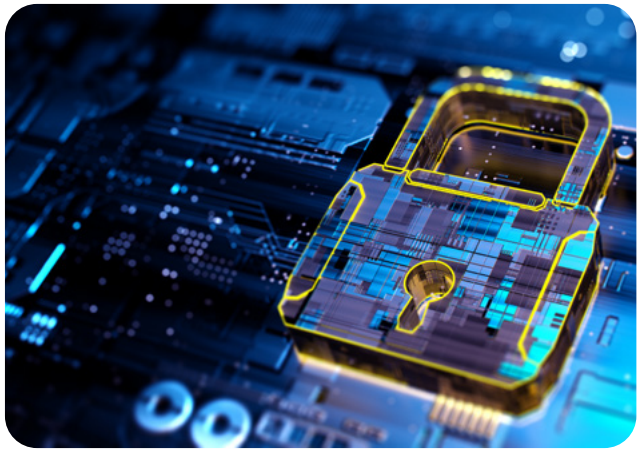
The research team intends to develop complete solutions for *authenticated group key establishment (AGKE)*, which will enable groups of users to exchange information and collaborate securely over open networks. These solutions aim to:

- offer strong security guarantees of the confidentiality of classical networks, taking into account the risks posed by quantum technology's potential to break traditional computer encryptions;
- look at protection mechanisms against attacks on the implementation-level

In order to accomplish these goals, the project brings together three important disciplines: Computer science, Engineering and Mathematics.

Deliverables

- The project aims to deliver *quantum-safe solutions* for AGKE with demonstrable provable security guarantees, including an adequate security model. To achieve this, the research team will:
  - Develop general techniques and concrete efficient protocols for quantum-safe AGKE. This includes a thorough cryptographic analysis to establish provable security guarantees and adequate modelling of potential adversary attacks with quantum computing technology.
  - Develop techniques for securely implementing quantum-safe AGKE protocols and provide actual secure implementations on different target platforms.
  - Develop efficient hybrid solutions for AGKE.



- The research team will make its theoretical findings available to the academia by publishing in international scientific and technological journals.
- The project is also following and contributing to the US National Institute of Standards and Technology (NIST) standardization of quantum-resistant public-key cryptographic algorithms.
- Throughout the project life-cycle young researchers will be provided with education and training.

Impact

- The results of the research will inform standardization efforts in the area of quantum-safe cryptography, e.g., the US National Institute of Standards and Technology (NIST) post-quantum cryptography standardization process;
- Models and solutions developed in this project could inspire a significant body of follow-up work, which might result in further efficiency improvements;
- Furthermore, the project will contribute to:
  - Increase the level of quantum security competencies and expertise exchange among the research communities of the participating nations;
  - Enhance the research and development area with special focus on cyber science and technology;
  - Advance the partnership between the research communities in cryptography and runtime verification;
  - Strengthen relations between the research communities of NATO and partner countries.