NATO

Science for Peace and Security (SPS) Programme

Secure communication in the quantum era: (group) key establishment

Christian Colombo, María Isabel González Vasco, Rainer Steinwandt, and Pavol Zajac

Project G5448

The Project

Leadership:

O. Grosek

Slovak U. of Technology in Bratislava, NPD

C. Colombo

U. of Malta, PPD

M. I. González Vasco

U. Rey Juan Carlos, Co-director Spain

R. Steinwandt

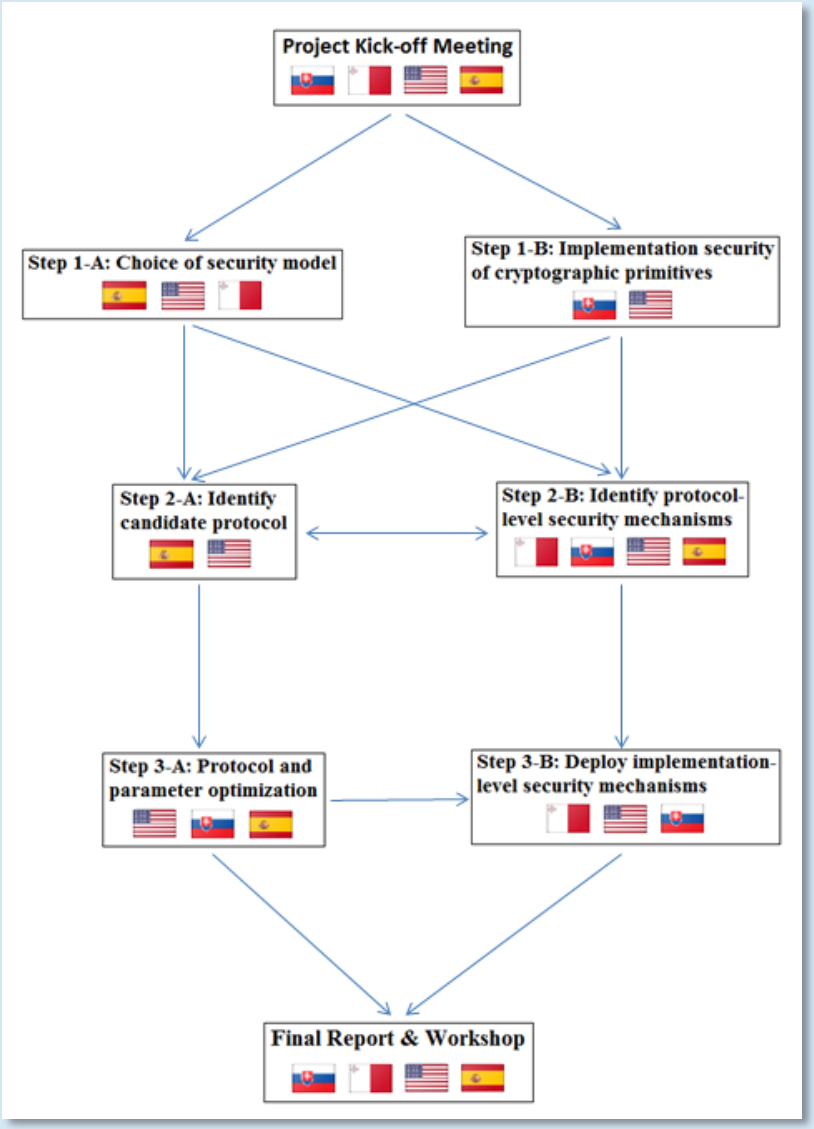
Florida Atlantic U. Co-director USA

Objective:

Enable groups of users to establish a cryptographically secured channel over insecure communication networks.

- Solution remains secure, if the adversary obtains access to a quantum computer.
- Solution offers resistance against attacks on the executed code at runtime.

Project Overview



Theoretical/Conceptual Thrust:

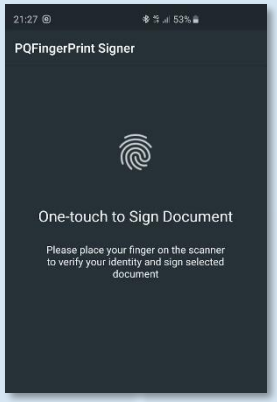
- (Quantum) cryptanalysis of tools to build cryptographically secure channels.
- Identify scalable group key establishment protocol with strong *provable* guarantees, taking into account implementation cost.

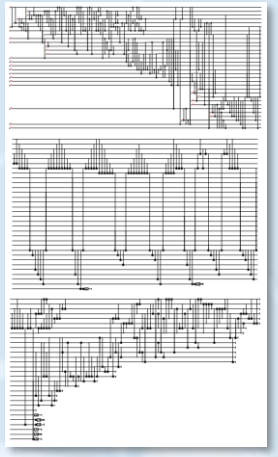
Implementation Thrust:

- Focus on software implementations, experiments with different platforms.
- Develop and apply runtime verification mechanisms to protect protocol execution, taking side-channels into account, too.

Project Outcome – Results

- **Advances in post-quantum cryptography:**
  - (quantum) cryptanalysis of encryption & signature primitives
    - ⇨ align with NIST post-quantum standardization effort
  - implementations on different platforms
    - ⇨ standard client-server, mobile
  - highly robust implementations
    - ⇨ leverage runtime verification
  - efficient group key establishment
    - ⇨ scalable design, emphasize simple crypto primitives
- **Training of students/future work force in quantum-safe cryptography**
    - ⇨ completed Naval Research Enterprise Internship Program
    - ⇨ presentation at AFRICACRYPT 2019
    - ⇨ serious implementations of post-quantum crypto





Project Outcome – Impact

- Influencing NIST's upcoming post-quantum cryptography standard
  - ⇨ project team represented in ongoing standardization effort
  - ⇨ synergy with ongoing evaluation of NIST candidates
  - ⇨ (re-)evaluating quantitative security margins needed

- Mature post-quantum crypto implementations
  - ⇨ available to end users and others

- Workforce development in quantum-safe cryptography
  - ⇨ NATO SPS participation as pathway to competitive internships

Way Forward

- Support for wide-scale deployment of post-quantum cryptography
  - ⇨ standardization, open source libraries
- Improve security research collaborations between crypto and physics
  - ⇨ improve security and analyze integration into protocol contexts
- Expand quantum cryptanalysis research
  - ⇨ full stack from quantum algorithms to quantum hardware