# SPS G5448
# Secure Communication in the Quantum Era

*Overview and progress*

Rainer Steinwandt
Florida Atlantic University

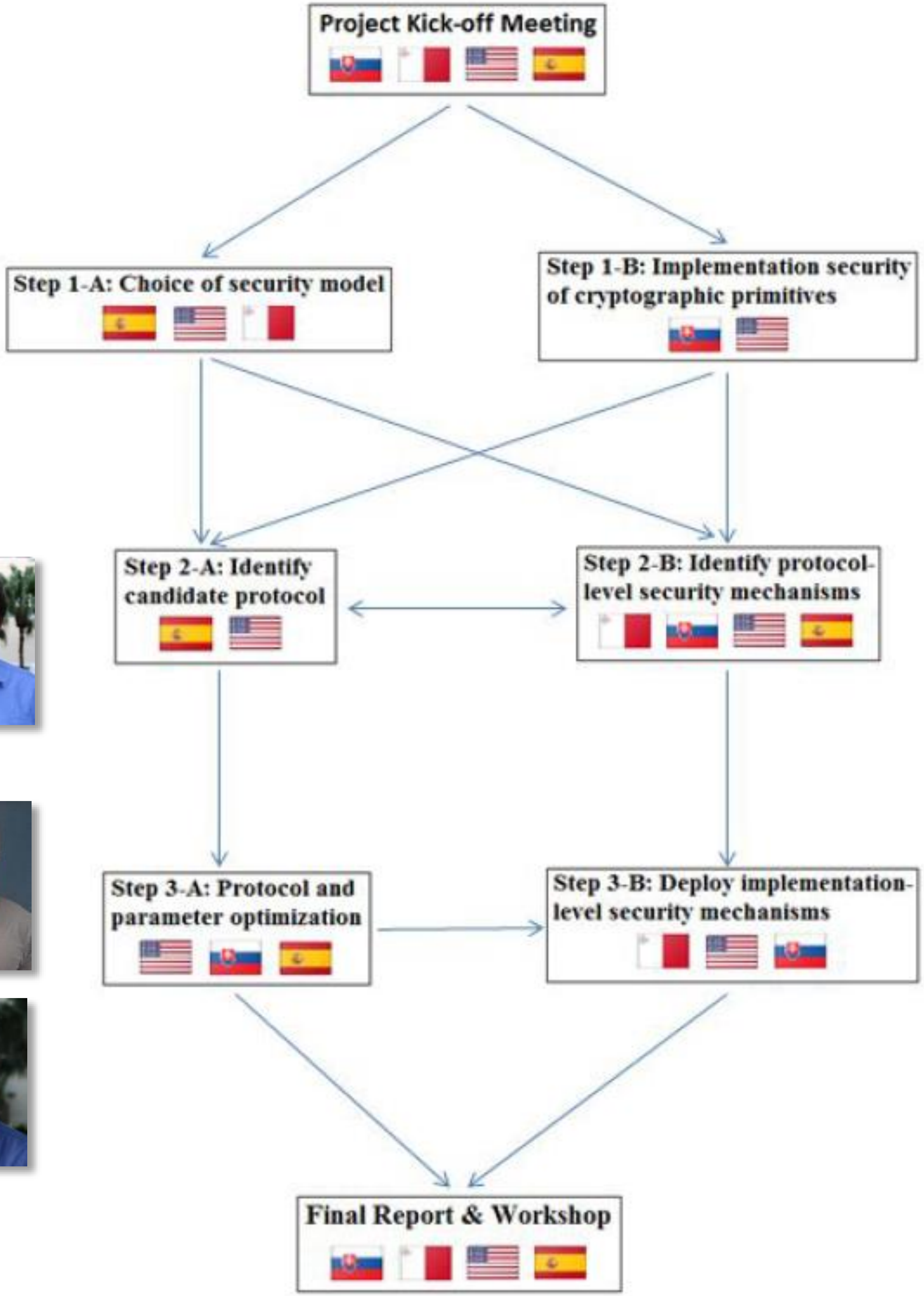
# Overall Structure of the Project

Current project activities at FAU focus on Steps 1-A and 2-A, including training of three Ph.D. students:

- **Floyd Johnson**: protocol models - MS presentation on provable security, possible improvement of efficiency of basic candidate

- **Sean Miller**: post-quantum key encapsulation – parameter choices, e.g., based on NewHope

- **Hai Pham**: improve available estimates on security baseline – quantum cost to recover AES key



Project Kick-off Meeting

Step 1-A: Choice of security model

Step 1-B: Implementation security of cryptographic primitives

Step 2-A: Identify candidate protocol

Step 2-B: Identify protocol-level security mechanisms

Step 3-A: Protocol and parameter optimization

Step 3-B: Deploy implementation-level security mechanisms

Final Report & Workshop

# Security baseline in a post-quantum setting

**NIST's approach in ongoing standardization effort in post-quantum cryptography:**

- Security strength categories based on resources needed to attack symmetric primitives.
- Two categories based on hash functions, three on AES:

> Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a $k$-bit key (e.g. AES$k$)

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

- AES cost estimates for quantum attack based on Grassl et al.'s work from PQCrypto 2016 (supported by NATO SPS project MD.SFPP 984520)

  ➡ improved quantum circuit by Almazrooie et al. 2018

**Ongoing work with Hai Pham and Brandon Langenberg (PQSecure Technologies):**

- New quantum circuit for S-box reduces #Toffoli gates by more than 87%, simultaneously also reducing #Clifford gates and #qubits.
- Revise cost estimate for Grover attack against AES.

# Protocol-design considerations

- Only post-quantum primitives where efficient (NIST competition) candidates are available

  ⇨ current candidate: black-box **key encapsulation** (e.g., based on NewHope)

- Try to use simple authentication primitives that enable clear interface to runtime verification

  ⇨ passwords and (one-time) **MAC** rather than post-quantum signatures?

  ⇨ any good use in our setting for ephemeral pre-quantum signatures?

- Communication topology and cost: current candidate – a collaborative effort with Spanish project partner – uses **star topology**

  ⇨ any cost benefit through adopting more general tree-based topology?

**Next steps:**

- Establish provable security guarantee for at least one candidate protocol.
- Clarify interface of candidate protocol with runtime verification.
- Clarify parameter needs for this candidate protocol.

# Increasing visibility and parameter confidence

- One of FAU's project team members (Edoardo Persichetti) co-authors three (of the 26) Round 2 candidates in NIST's post-quantum standardization effort.

- Three of FAU's project team members are involved in NIST award 60NANB18D217 "A Platform for the evaluation of post-quantum primitives" which is in the process of setting up a wiki platform to host
  - information on the security status of NIST candidates and
  - (small-scale) challenges for candidates/underlying problems

  Announcement of upcoming wiki at Oxford Post-Quantum Cryptography Workshop indicated strong interest

  ⇨ natural synergy for selecting right (post-quantum key encapsulation) primitive for our protocol need

**Plan:** Collaborate with wiki effort through this project, thereby

- increasing visibility of the project and
- obtain robust post-quantum cryptographic primitive with solid parameter choice