Implementation security of cryptographic primitives

Kick-off meeting

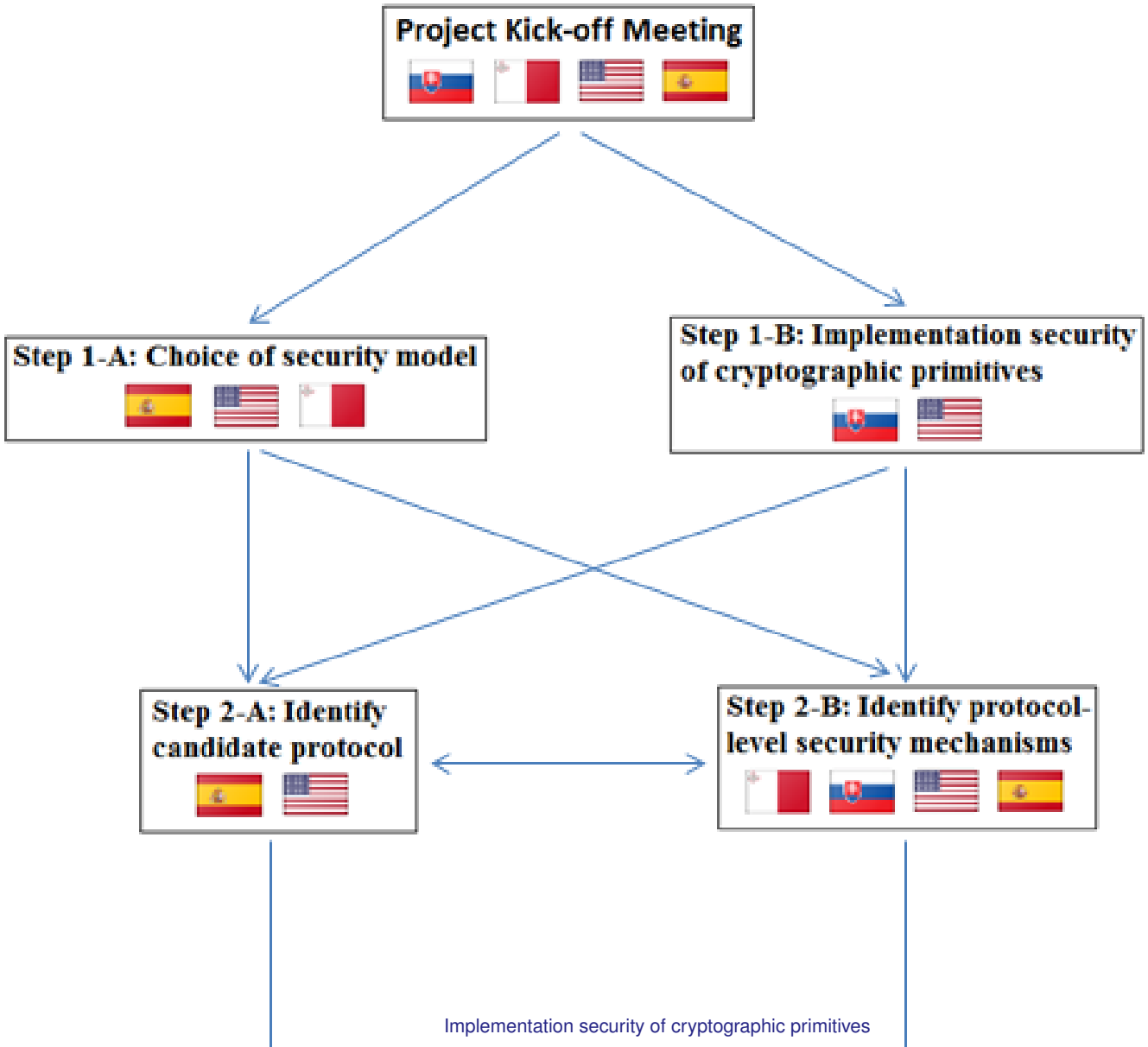
Secure communication in the quantum era
SPS Project Number: G5448

O. Grošek, **Pavol Zajac**

Institute of Computer Science and Mathematics
Slovak University of Technology

October 01, 2018

Project plan



Implementation security of cryptographic primitives

Main goal: to identify basic building blocks (like signature schemes) available which can effectively be protected against implementation-level attacks.

Need to review primitives of interest (NIST competition):

- hash-based signatures,
- code-based encryption (and signatures?)
- lattice-based constructions

Implementation security of cryptographic primitives

Primitives suitable for application in AGKEs:

- can support a selected type of protocol (steps),
- recommended parameters and key sizes/message sizes,
- speed of basic operations (including key generation),
- can be protected against side-channel attacks.

Deliverables (D2)

Implementation guidelines for side-channel resistant quantum-safe signing and for realizing basic operations as occurring in a quantum-safe 2-party key establishment (e.g., with a key encapsulation mechanism).

Discussion on deliverables

- D2: Guideline formal aspects (web-page/article/technical report).
- D2: Guideline contents proposal:
  - Review some well-known secure protocols that use generic/replaceable primitives (not DH dependent).
  - Overview of the NIST candidates and their classification with respect to required primitives.
  - Assessment/literature review of side-channel resistance of selected candidates.
- D2: Which *2-party*/*multiparty* key establishment protocol(s) to focus on (overlap with Step 2A)?
- D2: Make an overview of all NIST candidates or focus on some leaders?

Technical discussion for D2

Technical issues:

- research team,
- deliverable dead-line: 3q of year 2 (end of june 2020?),
- content sharing for collaboration,
- dependencies between project phases/deliverables,
- possible scientific/dissemination outputs (review articles? conference/workshop presentations?).