QUANTUM SAFE AUTHENTICATED GROUP KEY ESTABLISHMENT

NATO SPS programme- Project Number: G5448

Project Meeting, April 2nd, 2019

María Isabel González Vasco

URJC

NATO OTAN

URJC team- Spain

Manuel Arrayás,
Associate Prof. Electromagnetism,
María I. González Vasco,
Associate Prof. Applied Mathematics
Angel L. Pérez del Pozo,
Assistant Prof., Applied Mathematics
Jose L. Trueba
Associate Prof. Electromagnetism

TOWARDS SECURE POST-QUANTUM GROUP KEE AGREEMENT

URJC

NATO OTAN

PROGRESS REPORT: ACTIVITIES IN SPAIN

- Research work in progress
  - Model for secure PQ-GKE (main part of this presentation)
- Dissemination effords

- Involvement of students
  - Report on attacks on post-quantum proposals (WalnutDSA)

URJC

NATO OTAN

POST-QUANTUM GROUP KEY ESTABLISHMET

Main focus for the Spanish team

URJC

NATO OTAN

GKE: THE STARTING POINT FOR ENABLING SECURE COMMUNICATION

A priori-shared secrets are needed for many cryptographic tasks

"start up a secure session"
"stablish a secure channel "

URJC

NATO OTAN

GKE: THE STARTING POINT FOR ENABLING SECURE COMMUNICATION

A priori-shared secrets are needed for many cryptographic tasks

URJC

NATO OTAN

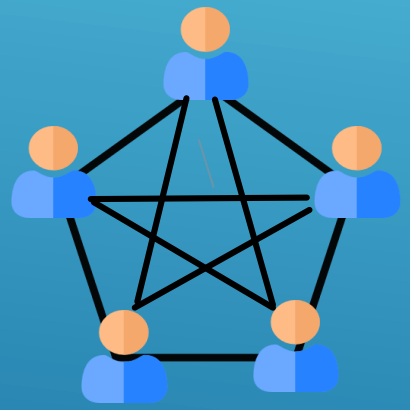
GKE: THE STARTING POINT FOR ENABLING SECURE COMMUNICATION

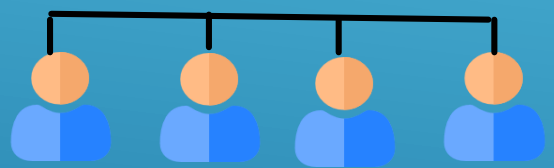
A priori-shared secrets are needed for many cryptographic tasks

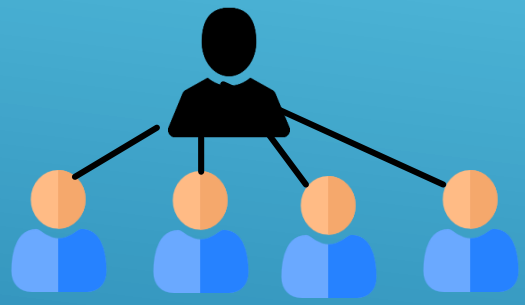
URJC

NATO OTAN

GKE: DIFFERENT SCENARIOS







- User roles (identical, jerarchical, etc.)
- Communication network (peer-to-peer, broadcast,..)

URJC

NATO OTAN

PROJECT STEP 1-A :

Choice/Design of security model form GKE capturing post-quantum attacks

URJC

NATO OTAN

GENERIC GOALS (FOR GROUP APPLICATIONS)

- Correctness
- Availability
- Efficiency
- Security : confidenciality, authentication, access control, anonymity

→ all can be attained through GKE

URJC

NATO OTAN

GKE: SECURITY GOALS

- Key confidenciality/key secrecy: (secrecy, freshness, Independence, randomness, indistinguishability…)
- Authentication
- Key confirmation/Key integrity

URJC

NATO OTAN

GKE: SECURITY MODEL

Formal description of adversarial capacities:

- Can they inject messages, or just eavesdropp?
- Can they corrupt group members? In what sense?
- Can they attack different (concurrent) sessions?
- Can they obtain previously agreed keys?

Further, in a post-quantum scenario we need to describe the adversarial access to quantum technologies (channels, computing, storage..)

Typical modelling of adversarial capacities is done through Oracle formulation

URJC

NATO OTAN

THIS PROJECT: MODELLING SCENARIO

- Security model: Quantum-Future
  - During the protocol execution: classical adversaries
  - After the protocol execution: quantum adversaries
  - Users are always classical

- Advantages: modelling quantum attacks in a non-restrictive way, to be able to derive efficient solutions

- Rationale:

  - Quantum attacks are not considered at the execution time → standard (not post-quantum) authentication means can be used (thus we avoid"expensive" PQ signatures)
  - The resulting keys will remain secure once quantum adversaries are present, if forward security is attained by our design

URJC

NATO OTAN

FOCUSING ON GKE: SECURITY GOALS

- We will use Oracle-modelling to capture adversarial capacities, focusing on attaining two properties:
  - Key secrecy (defined in a *real-or random* fashion: adversaries should not be able to tell apart a real key from one chosen at random from the key space)
  - Forward security (leakage of authentication keys has no inpact in previously agreed session keys)

URJC

NATO OTAN

FURTHER : AUTHENTICATION

- Authentication;
  - Group: messages are recognized as sent by someone from the group
    → attained typically through passwords
  - User: messages are recognized as sent by a specific user inside the group
    → attained typically through digital signatures

URJC

NATO OTAN

TOWARDS PROJECT STEP 2-A :

Design Tools :

- Classical authentication methods (MACs, digital signatures)
- Post-quantum tools (KEMs)

URJC

NATO OTAN

EXPECTED OUTCOME (D3)
2ND YR, 4TH QR (JULY/SEPT 2020)

- Detailed security model
- High level description of a generic protocol
- Detailed constructions (based on different primitives)
- Security analysis (theoretical/practical/using run-time verification techniques)
- Implementation guidance

URJC

NATO OTAN

EXPECTED OUTCOME (D3)
2ND YR, 4TH QR (JULY/SEPT 2020)

- **Detailed security model**
- **High level description of a generic protocol**
- Detailed constructions (based on different primitives)
- Security analysis (theoretical/practical/using run-time verification techniques)
- Implementation guidance

URJC

NATO OTAN

THANK YOU