SECURE COMMUNICATION IN THE QUANTUM ERA

Contribution of the Spanish Team

María Isabel González Vasco

NATO SPS programme- Project Number: G5448
Project Meeting, March, 2020

SUMARY OF OUTCOMES

URJC

- Actions:
  - Internal meetings
  - Project meetings (including end users) at URJC
  - Boosting interaction with the other institutions involved in the Project
- Main Contributions:
  - Step 2-A: Identify candidate protocol
  - Step 2-B: Identify protocol-level security mechanisms
  - Final Report: comparison to state of the art alternatives

- Dissemination:
  - Scientific Publication
  - Outreach (general public)

Actions

MAIN CONTRIBUTIONS

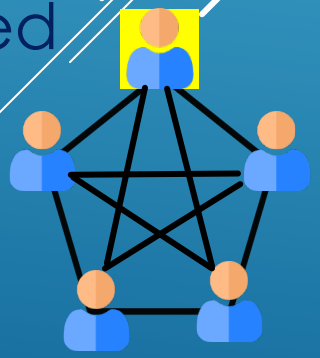
- Active cooperation with US Team towards design and análisis of Future-Quantum GAKE
- Coordination with the Slovak partners (final meeting in Madrid, May 2022) towards final chat application

- Towards the Final Report:
  - Analysis of state of the art related work, in particular, throught study of alternatives towards Post Quantum GAKE

The protocol

- TOOLS
  - IND-CPA post-quantum KEM (Kyber, Saber, NTRU…)
  - UF-CMVA message authentication code

- DESIGN RATIONALE
  - Key transport: designated special user U_0 fixes key
  - Authentication: password based; Diffie-Hellman keys are exchanged from which symmetric MAC keys are derived

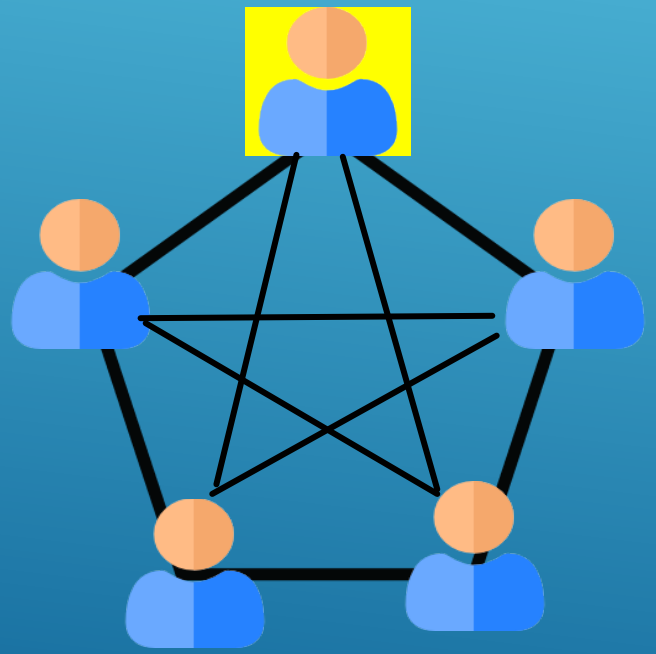


The protocol - unauthenticated version

KEY TRANSPORT

- U_0 fixes sesión key sk:=k
- For each j =1,…,n, U_0
  - Runs Encaps(pk_j), getting (c_j , k_j)
  - d_j : = k ⊕ k_j
  - sends M_j:= (d_j , c_j)

The protocol - unauthenticated version



KEY ESTABLISHMENT

- U_0 sets

$$ssk_0 = k$$

- For i =1,…,n, U_i sets

$$ssk_i = d_i \oplus k_i$$

The protocol - Adding authentication

Two-party Diffie-Hellman key Exchange protocols are executed among all pairs of users (base element –pw)

The protocol - Adding authentication

Two-party Diffie-Hellman key Exchange protocols are executed among all pairs of users (base element –pw)

1. User U_i selects ephemeral β_i and publishes $g_i = pw^{\beta i}$
2. Users U_i and U_i share a group element $g_{ij} = pw^{\beta i \beta j}$
3. Two-party symmetric MAC keys are extracted from the group elements
4. MAC tags can be apehended to each message

Pos/Cons

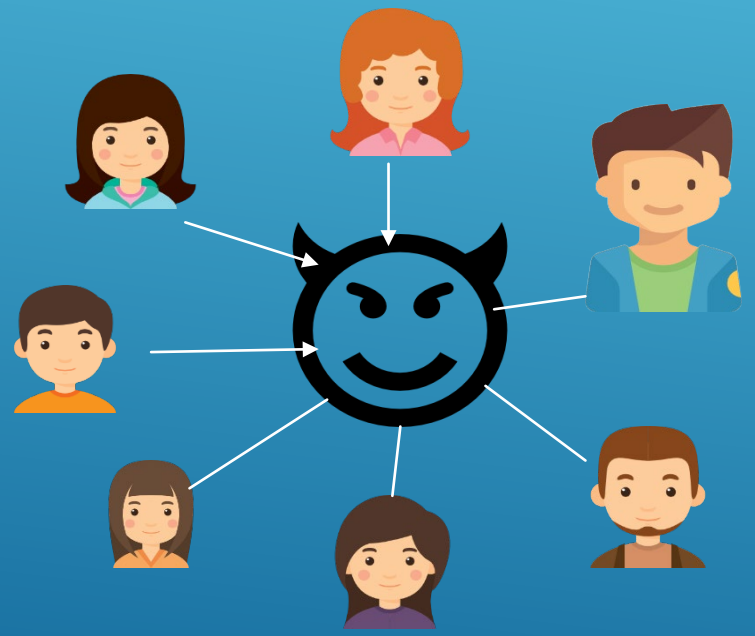
- Password authentication
- “cheap” PQ primitives (MAC + KEM)

- Key Transport (full trust in U_0)
- If authentication is required:
  - High communication complexity
  - “only” Future Quantum

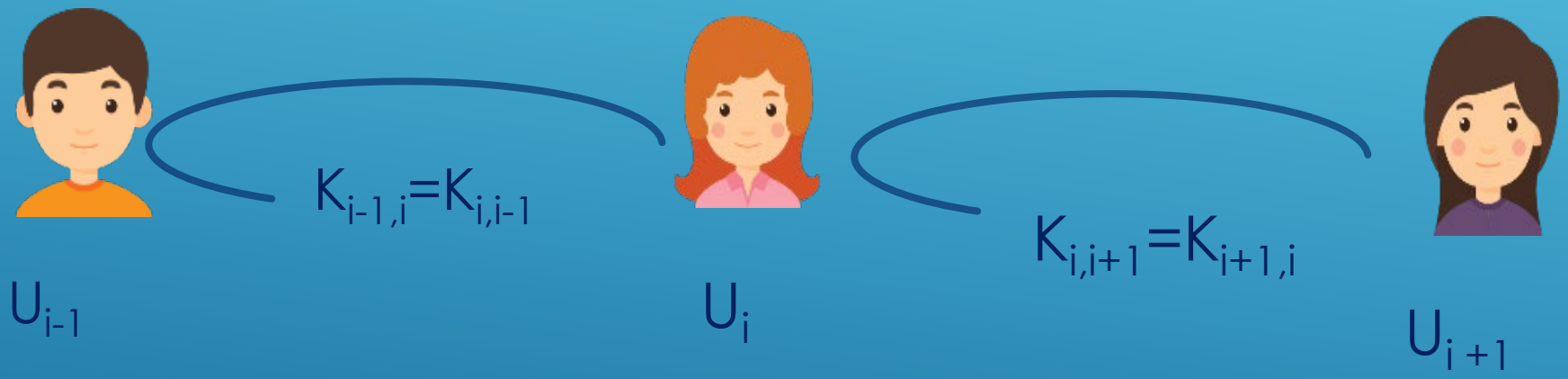
Can we get fully PQ?

A compiled solution

Users are assumed to be in a ring-network



Round 1 [2-AKE]



Round 2 [COMMITMENT]

Each user U_i

- Sets

$$X_i = K_{i,i+1} \oplus K_{i,i-1}$$

Round 2 [COMMITMENT]

Each user U_i

- Sets

$$X_i = K_{i,i+1} \oplus K_{i,i-1}$$

- Commits to this value with randomness r_i

$$C_i = Com(i, X_i, r_i)$$

Round 2 [COMMITMENT]

Each user U_i

- Sets

$$X_i = K_{i,i+1} \oplus K_{i,i-1}$$

- Commits to this value with randomness r_i

$$C_i = Com(i, X_i, r_i)$$

- Sends $M_i^2 := (i, C_i)$

Round 3 [FINAL DISTRIBUTION AND KEY COMPUTATION]

Each user U_i

- Sends

$$M^3_i := (i, X_i, r_i)$$

Round 3 [FINAL DISTRIBUTION AND KEY COMPUTATION]

Each user U_i

- Sends

$$M^3_i := (i, X_i, r_i)$$

- Checks:
  - $X_o \oplus X_1 \oplus \ldots \oplus X_{n-1} = 0$
  - commitments from Round 2

Round 3 [FINAL DISTRIBUTION AND KEY COMPUTATION]

Each user U_i

- Sends

$$M^3_i := (i, X_i, r_i)$$

- Checks:
  - $X_o \oplus X_1 \oplus \ldots \oplus X_{n-1} = 0$
  - commitments from Round 2

- If OK, compute two party keys and set

$$K = F(K_{o,1}; K_{1,2}; \ldots; K_{n-1,0})$$

Pos/Cons

- Authentication - inherited from (2-party) AKE
- Proven secure and implemented from many different PQ KEMS (Kyber/NTRU/Saber/McEliece)
- Contributiveness

Pos/Cons

- Authentication - inherited from (2-party) AKE
- Proven secure and implemented from many different PQ KEMS (Kyber/NTRU/Saber/McEliece)
- Contributiveness

- Complete newtork (or broadcast cannel)
- Ring configuration (no robustness to node failures)
- High communication complexity

Dissemination

OUTREACH

SCIENTIFIC PRESENTATIONs

M. Marriaga: *Post-quantum Vs Quantum Future: The case of Group Key Exchange*. Talk at the V Congreso de Jóvenes Investigadores de la RSME, January 2020.

M.I. González Vasco, Àngel L. Pérez del Pozo, Rainer Steinwandt. *Group Key Establishment in a Quantum-Future Scenario*, 2022 AWM Research Symposium, Minessota, USA, 2022.

M.I. González Vasco, Àngel L. Pérez del Pozo, Rainer Steinwandt. *Intercambio de clave en grupo en la era cuántica.* I Encuentro QTEC (Tecnologías Cuánticas), Centro Criptológico Nacional, Madrid, 2022.

Dissemination

OUTREACH

PUBLICATIONS

1. M.I. González Vasco, A.L. Pérez del Pozo and C. Soriente. *A key for John Doe: modeling and designing Anonymous Password-Authenticated Key Exchange protocols* . IEEE Transactions on Dependable and Secure Computing, Volume 18, Issue 3, 2021.

2. Arrayás, M., Trueba, J.L., Uriarte, C. et al. Design of a system for controlling a levitating sphere in superfluid 3He at extremely low temperatures. Sci Rep 11, 20069, 2021.

3. C. González, M.I. González Vasco, F. Johnson, and A.L. Pérez del Pozo. *An Attack on Zawadzki's Quantum Authentication Scheme*. Entropy, 23(4), 38, 2021.

4. A.I. González Tablas, M.I. González Vasco, I. Cascos and A. Planet Palomino. *Shuffle, Cut, and Learn: Crypto Go, a Card Game for Teaching Cryptography* Mathematics, 8.,(11), 1993, 2020.

5. M.I. González Vasco, J.I. Escribano Pablos, M.E. Marriaga and A.L. Pérez del Pozo, *Compiled Constructions towards Post-Quantum Group Key Exchange: A Design from Kyber*. Mathematics, 8, 1853, 2020.

Dissemination

PUBLICATIONS

6. M.I. González Vasco, A. Pérez del Pozo and R. Steinwandt. *Group Key Establishment in a Quantum-Future Scenario*. Informatica, Vol 31, 4, pp. 751-768, 2020.

7. J.-M. Bohli, M.I. González Vasco and R. Steinwandt. *Building Group Key Establishment on Group Theory: A Modular Approach*. Symmetry, *12*(2), 197, 2020.

8. M.I. González Vasco. *El enemigo a las puertas: avances en criptografía clásica para un mundo cuántico*. Gaceta de la RSME, Vol 23 (1), pp. 187—204, 2020.

PREPRINTS

1. J.I. Escribano Pablos and M.I. González Vasco. *Secure PostQuantum Group Key Exchange: Implementing a Solution Based on Kyber.*

2. J.I. Escribano Pablos, M.E. Marriaga, and A. L. Pérez del Pozo. *Design and Implementation of a Post-Quantum Group Authenticated Key Exchange protocol with the LibOQS library: a comparative performance analysis from Classic McEliece, Kyber, NTRU, and Saber*“

THANK YOU

Icons made by Freepik from www.flaticon.com