PROGRESS IN FUTURE-QUANTUM GROUP KEY ESTABLISHMENT PROTOCOLS

Overview and Progress

María Isabel González Vasco

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

M2: PROJECT AGENDA AT URJC

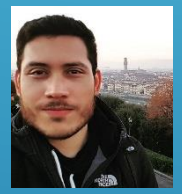
- Actions:
  - Internal meetings
  - Project meeting (including end users) at URJC
  - Boosting interaction with the other institutions involved in the Project
- Scientific progress:
  - Step 2-A: Identify candidate protocol
  - Step 2-B: Identify protocol-level security mechanisms
- Dissemination:
  - Scientific Publication
  - Outreach (general public)

Actions

INTERNAL MEETINGS AT URJC







- Learning specifics of NIST post-quantum proposals

(this time, focusing on group-theoretical scheme)

- Training the new team member (Misael Marriaga)

(seminars on group key Exchange and security notions for post-quantum constructions)

1. Publications :
    1. M.I. González Vasco, José Ignacio Escribano Pablos, Misael Enrique Marriaga and Ángel Luis Pérez del Pozo) *The Cracking of WalnutDSA: A Survey*, Symmetry 2019, 11(9), 1072, 2019
    2. 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.
2. Talk by M. Marriaga delivered at RSME meeting (January 2020)

Actions

PROJECT MEETING AT URJC (SEPT 2020)

- Getting together with end-users
- Started concrete collaboration with implementers/run time verification teams

Outreach: video, URJC news, BBC world.

1. **A Project of 'Science for Peace and Security' Program Held Its Third Session at the University**. Article published on the official website of Universidad Rey Juan Carlos, September 25, 2019.
2. **Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen.** Analía Llorente, BBC News Mundo. 26 December 2019.
3. **Secure Communication in the Quantum Era**, TV URJC video spot. 24.1.2020

Actions

INTERACTION WITH FAU/STU/UM

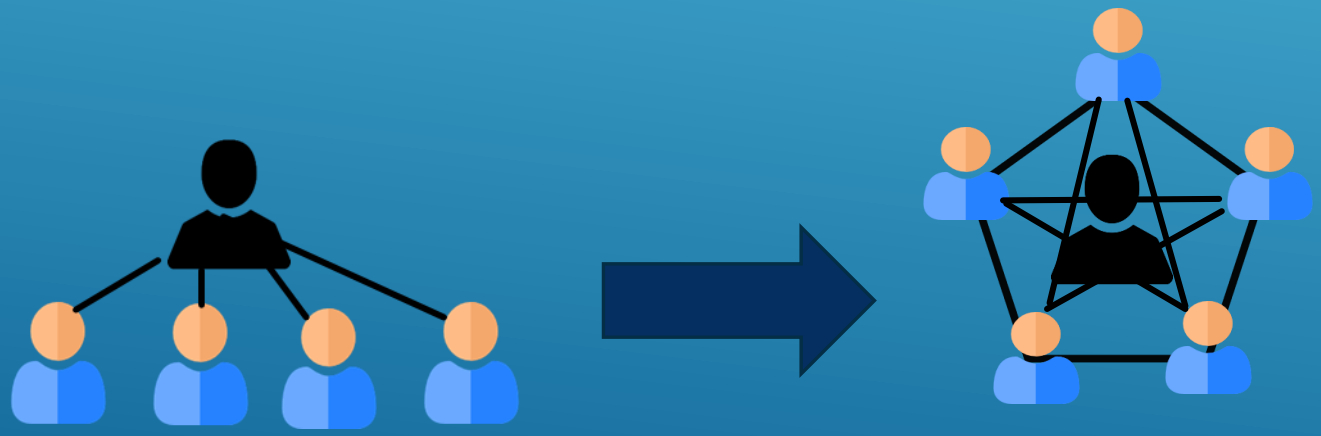
- Skype meetings and email discussion with
  - FAU members: protocol design
  - STU/UM: implementation

- Floyd Johnson visited URJC (4 weeks)
  - Training on group key establishment
  - Joint exploration of quantum protocols for identification (preprint in progress)

Scientific Progress

STEP 2-A

- **Identify candidate protocol**
  - Decided for a not-fully symmetric configuration of users (i.e., a central user plays special role, yet no special trust assumptions needed!
  - Decided for deviating from a compiled construction (still, we build on a two party post-quantum tool – a KEM)



Scientific Progress

STEP 2-A

- Our construction:
  - Uses passwords for authentication
  - Can be implemented with diferent (post-quantum) KEMs
  - Needs only two rounds of communication
  - Can be modified to be contributory

1. Publications:

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

2. Preprint including protocol design and security proof (joint paper under submission) M.I. González Vasco, A.L. Pérez del Pozo, R. Steinwandt. Group Key Establishment in a Quantum Future Scenario

Scientific Progress

STEP 2-B

- **Identify protocol-level security mechanism**
  - **Key-privacy** is obtained from (IND-CPA) security of the underlying post-quantum KEM
  - **Authentication** comes from a symmetric tool (MAC) –and DDH!!
  - **Quantum Oracle Call** capture the (limited) adversarial access to quantum computation

1. Publications:

   1. Anonymous PAKE : 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, to appear.

   2. AMCS M.I. González Vasco, J.M. Bohli and R. Steinwandt) *Password Authenticated Group Key Establishment from Smooth Projective Hash Functions*. International Journal of Applied Mathematics and Computer Science (AMCS), Vol. 29, No. 4, 797–815, 2019.

Dissemination

SCIENTIFIC PUBLICATIONS

- M.I. González Vasco, J.-M. Bohli and R. Steinwandt. *Building Group Key Establishment on Group Theory: A Modular Approach*. Symmetry, *12*(2), 197, 2020.
- 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, to appear.
- M.I. González Vasco, José Ignacio Escribano Pablos, Misael Enrique Marriaga and Ángel Luis Pérez del Pozo) *The Cracking of WalnutDSA: A Survey*, Symmetry 2019, 11(9), 1072, 2019.
- M.I. González Vasco, J.M. Bohli and R. Steinwandt. *Password Authenticated Group Key Establishment from Smooth Projective Hash Functions*. International Journal of Applied Mathematics and Computer Science (AMCS), Vol. 29, No. 4, 797–815, 2019.

PREPRINTS

- M.I. González Vasco, A.L. Pérez del Pozo, R. Steinwandt. *Group Key Establishment in a Quantum Future Scenario*
- F. Johson, C. González, M.I. González-Vasco, A.L. Perez del Pozo. *Concerning Quantum Identity Authentication without entanglement.*

Dissemination

OUTREACH

SCIENTIFIC PRESENTATION

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.

PUBLICATION

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.

GENERAL PUBLIC

- A Project of 'Science for Peace and Security' Program Held Its Third Session at the University. Article published on the official website of Universidad Rey Juan Carlos, September 25, 2019.

- Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen. Analía Llorente, BBC News Mundo. 26 December 2019.
- Secure Communication in the Quantum Era, TV URJC video spot. 24.1.2020

THANK YOU