“Secure Communication in the Quantum Era”

Science For Peace and Security
Project G5448

Come Join us at the Open Session

September 26th, 2019
CAMPUS DE MÓSTOLES, URJC,
SALA DE GRADOS, EDIFICIO DEPARTAMENTAL II

9:30 OPENING
10:15 COFFEE BREAK & GROUP PICTURE
10:54-11:00 Introducing the Spanish National Cryptologic Center, CCN

11:00- 12:00 MORNING SESSION

Milestone 2. Project goals and outcome, O. Grošek , STU

A smaller quantum circuit for AES: simplifying a Grover-based key search, R. Steinwandt. FAU

GKE protocols in a Quantum-Future scenario, M.I. G. Vasco, URJC

14:30- 16:30 AFTERNOON SESSION

Towards a practical application of runtime verification techniques for security protocols, C. Colombo, UM

New PQ signature scheme from block ciphers, P. Zajac , STU

A Group Key Exchange Scheme from PQCrypto 2019, T. Fabsic, STU

PQ crypto in TLS-like setting, P. Spacek, STU.