



Science for Peace and Security (SPS) Programme meeting

Universidad Rey Juan Carlos

24-26 September 2019

24 September 2019

PROGRAMME

09:30	ARRIVAL AND REGISTRATION
10:00	Business Meeting on G5448: "Secure Communication in the Quantum Era"
11:00	COFFEE BREAK
10:30	Business Meeting on G5448: "Secure Communication in the Quantum Era"
12:30	LUNCH BREAK
14:00	Close-up of Day 1

25 September 2019

PROGRAMME

09:30	ARRIVAL AND REGISTRATION
10:00	Business Meeting on G5448: "Secure Communication in the Quantum Era"
11:00	COFFEE BREAK
10:30	Business Meeting on G5448: "Secure Communication in the Quantum Era"
12:30	LUNCH BREAK
14:00	Close-up of Day 2



26 September 2019 – Public Session

PROGRAMME

09:30	Opening session <ul style="list-style-type: none">• Institutional represent. URJC• Dr. Karol Nemoga, SPS Project evaluator, NATO
10:15	COFFEE BREAK & GROUP PHOTO
10:45	End user talk: “Introducing the Spanish National Cryptologic Centre (CCN)”, by Ursula CCN.
11:00 12:30	Meeting on G5448 “Secure Communication in the Quantum Era” <ul style="list-style-type: none">• O. Grošek: Milestone 2. Project goals and outcomes.• R. Steinwandt: A smaller quantum circuit for AES: simplifying a Grover-based key search• M. I. Gonzalez Vasco: GKE protocols in a Quantum-Future scenario
12:30- 14:30	LUNCH BREAK
14:30- 16:30	Meeting on G5448 “Secure Communication in the Quantum Era” <ul style="list-style-type: none">• C. Colombo: Toward a practical application of runtime verification techniques for security protocols• P. Zajac: New PQ signature scheme from block ciphers• T. Fabsic: A Group Key Exchange Scheme from PQCrypto 2019• P. Spacek: PQ crypto in TLS-like setting
16:30	Closing of public session
17:00	Meeting on G5448 “Secure Communication in the Quantum Era” <ul style="list-style-type: none">• R. Steiwnandt: Report on the NATO SPS CLUSTER WORKSHOP ON KEY PRIORITY AREA ADVANCED TECHNOLOGIES (Leuven, Belgium - 17-18 September 2019)