IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advances in Space-based Communication Systems and Services, Part 2 (3)

Author: Mr. Federico Berra
University of Padova, Italy, fede.berra@hotmail.it

Dr. Costantino Agnesi
Università degli Studi di Padova, Italy, agnesi@dei.unipd.it
Mrs. Ilektra Karakosta-Amarantidou
Università degli Studi di Padova, Italy, ilektra.karakostaamarantidou@unipd.it
Dr. Marco Avesani
Università degli Studi di Padova, Italy, avesani@dei.unipd.it
Mr. Matías Rubén Bolaños Wagner
Università degli Studi di Padova, Italy, matiasruben.bolanoswagner@studenti.unipd.it
Mr. Alberto De Toni
Università degli Studi di Padova, Italy, alberto.detoni.1@studenti.unipd.it
Dr. Andrea Stanco
University of Padova, Italy, andrea.stanco@unipd.it
Dr. Francesco Picciariello
DEI - University of Padova and INFM - CNR LUXOR, Italy, francesco.piccia@live.it
Dr. Francesco Vedovato
Università degli Studi di Padova, Italy, vedovatofr@dei.unipd.it
Prof. Nicola Laurenti
Università degli Studi di Padova, Italy, nil@dei.unipd.it
Prof. Giuseppe Vallone
Università degli Studi di Padova, Italy, vallone@dei.unipd.it
Prof. Paolo Villoresi
Università degli Studi di Padova, Italy, paolo.villoresi@dei.unipd.it

HIGH-SPEED SOURCE FOR SATELLITE QUANTUM KEY DISTRIBUTION

Abstract

Quantum key distribution (QKD) is a technique used to establish a secure communication channel between two parties, known as Alice and Bob. The security of QKD is based on the principles of quantum mechanics, which allow for the creation of a shared secret key that cannot be intercepted by an eavesdropper, known as Eve. The shared secret key can then be used to encrypt and decrypt messages sent between Alice and Bob. QKD is a promising technology for secure communication because it offers unconditional security, meaning that the security of communication is guaranteed by the laws of physics. This is in contrast to classical encryption methods, which rely on the computational difficulty of certain mathematical problems and can be theoretically broken with enough computing power. QKD is performed with an exchange of qubits that are typically encoded into single photon-level pulses that are limiting the maximum distance of communication in the terrestrial network. Satellite links could offer a solution for enabling communication over long distances by taking advantage of the free-space channel's low attenuation and satellite mobility. The QUANGO project aims to design a constellation of the low-earth orbit of 12U-CubeSat satellites with combined capabilities for communication secured by QKD and for

5G connection for the Internet of Things (IoT), as well as to develop payloads, sub-systems, and ground stations for such a network and to determine the viability of its implementation. Within the project QUANGO, we report on the development of a high-speed breadboard-level QKD source realized up to TRL 4 to be evolved into a 3U engineering model, and an optical ground station with a 40 mm German mount telescope able to collect the optical signal with a pointing acquisition and tracking system and analyze it through single-mode fiber injection. The source was developed in two different wavelengths compatible with TELECOM standard: at 800 nm to reduce the divergence, and at 1550 nm compatible with daylight communication. Both sources were realized with an iPOGNAC-based modular scheme that simplifies its development, testing, and qualification, especially for space missions. All the components used for their realization were space COTS to reduce the space qualification costs.