PROCEEDINGS OF SPIE

Advanced Photon Counting Techniques VIII

Mark A. Itzler
Joe C. Campbell
Editors

7–8 May 2014
Baltimore, Maryland, United States

Sponsored and Published by
SPIE

Volume 9114

Proceedings of SPIE 0277-786X, V. 9114

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

Advanced Photon Counting Techniques VIII, edited by Mark A. Itzler, Joe C. Campbell, Proc. of SPIE
Vol. 9114, 911401 · © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2072633

Please use the following format to cite material from this book:
Author(s), "Title of Paper," in *Advanced Photon Counting Techniques VIII*, edited by Mark A. Itzler, Joe C. Campbell, Proceedings of SPIE Vol. 9114 (SPIE, Bellingham, WA, 2014) Article CID Number.

ISSN: 0277-786X
ISBN: 9781628410518

Published by
SPIE
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone +1 360 676 3290 (Pacific Time) · Fax +1 360 647 1445
SPIE.org

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.

SPIE Digital Library
SPIEDigitalLibrary.org

Paper Numbering: Proceedings of SPIE follow an e-First publication model, with papers published first online and then in print and on CD-ROM. Papers are published as they are submitted and meet publication criteria. A unique, consistent, permanent citation identifier (CID) number is assigned to each article at the time of the first publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online, print, and electronic versions of the publication. SPIE uses a six-digit CID article numbering system in which:

- The first four digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B … 0Z, followed by 10-1Z, 20-2Z, etc.

The CID Number appears on each page of the manuscript. The complete citation is used on the first page, and an abbreviated version on subsequent pages. Numbers in the index correspond to the last two digits of the six-digit CID Number.

Contents

SUPERCONDUCTING SPDs I: FREE SPACE COMMUNICATIONS

QUANTUM COMMUNICATIONS

SINGLE-PHOTON IMAGING AND PHOTON-COUNTING ARRAYS

SINGLE-PHOTON LIDAR

SOLID-STATE PHOTOMULTIPLIERS

VISIBLE AND UV SINGLE-PHOTON COMMUNICATIONS

Conference Committee

Symposium Chair

David A. Whelan, Boeing Defense, Space, and Security (United States)

Symposium Co-chair

Wolfgang Schade, Technische Universität Clausthal (Germany) and Fraunhofer Heinrich-Hertz-Institut (Germany)

Conference Chair

Mark A. Itzler, Princeton Lightwave, Inc. (United States)

Conference Co-chair

Joe C. Campbell, University of Virginia (United States)

Conference Program Committee

Gerald S. Buller, Heriot-Watt University (United Kingdom)
Sergio Cova, Politecnico di Milano (Italy)
William H. Farr, Jet Propulsion Laboratory (United States)
Robert H. Hadfield, University of Glasgow (United Kingdom)
Majeed Hayat, The University of New Mexico (United States)
Michael A. Krainak, NASA Goddard Space Flight Center (United States)
Robert A. Lamb, SELEX Galileo Ltd. (United Kingdom)
K. Alex McIntosh, MIT Lincoln Laboratory (United States)
Alan L. Migdall, National Institute of Standards and Technology (United States)
Michael Wahl, PicoQuant GmbH (Germany)
Hugo Zbinden, University of Geneva (Switzerland)

Session Chairs

1 Superconducting SPDs I: Free Space Communications
Mark A. Itzler, Princeton Lightwave, Inc. (United States)

2 Superconducting SPDs II: Quantum Information Processing
Eric A. Dauler, MIT Lincoln Laboratory (United States)

3 Quantum Communications
Alan L. Migdall, National Institute of Standards and Technology (United States)

4 Single-Photon Imaging and Photon-Counting Arrays
Gerald S. Buller, Heriot-Watt University (United Kingdom)

5 Single-Photon Lidar
K. Alex McIntosh, MIT Lincoln Laboratory (United States)

6 Solid-State Photomultipliers
Joe C. Campbell, University of Virginia (United States)

7 Visible and UV Single-Photon Communications
Mark A. Itzler, Princeton Lightwave, Inc. (United States)

8 Novel Photon-Counting Technologies
Mark A. Itzler, Princeton Lightwave, Inc. (United States)

Progress towards implementation of a quantum communication receiver satellite

T. Jennewein, E. Choi, B. Higgins
Institute for Quantum Computing and the Department of Physics and Astronomy
University of Waterloo, 200 University Ave. W, Canada N2L 3G1

The secure distribution of cryptographic keys has always been a crucial element for the task of protecting and sharing important secrets. Today's algorithmic key distribution makes assumptions on the computing power of a possible hacker, which leads to fundamental problems for long-term security. Quantum key distribution (QKD) establishes highly secure keys between distant parties by using single photons to transmit each bit of the key. Since single photons behave according the laws of quantum mechanics they cannot be tapped, copied or directly measured without disturbance. The huge benefit for users of such systems is the peace of mind of knowing that any attack, manipulation or copying of the photons can be immediately detected and overcome. QKD solves the long-standing problem of securely transporting cryptographic keys between distant locations. Even if they were to be transmitted across hostile territory, their integrity could be unambiguously verified upon receipt.

Ground-based QKD systems are commercially available today. However, these current systems can only cover distances of up to 200 km due to photon absorption in fiber optic cables. In principle, quantum repeaters would allow the concatenation of several shorter quantum links and thereby overcome the limitations of direct long-distance quantum transmissions, and much research is devoted to solving technical hurdles that prevent deployment of these devices outside laboratory settings. Satellite-based quantum communication systems, however offer an approach for surpassing distance limitations even with today's technology, and a truly global network for quantum communication becomes feasible in the near-term (Figure 1).

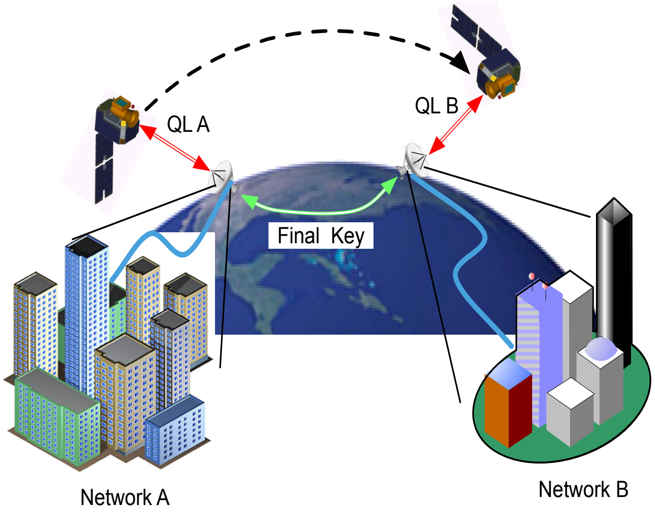

Figure 1: A satellite can be used as a trusted node to bridge the large distance gap between two city-wide networks.

Over the past three years, our group has been working with industry partners to advance a proposed microsatellite mission called QEYSSat (Quantum EncrYption and Science Satellite) through a series of conceptual and technical studies funded primarily by the Canadian Space Agency (CSA) [1]. QEYSSat's mission objectives are to demonstrate the generation of encryption keys through the creation of quantum links between ground and space, and also to conduct fundamental science tests of long-distance quantum entanglement [2].

The quantum signals are generated in photon sources located on the ground. An optical transmitter on the ground will point the beam of photons towards the satellite. One important aspect of this mission concept is to keep the complex source technologies on the ground and ensure the satellite is simple and cost-effective. It also allows the quantum link to be implemented using various different types of quantum sources, including entangled photons and weak coherent pulses. Placing the quantum receiver in space, however, poses some additional technical challenges. The expected link losses will be higher for the uplink than for a downlink. In addition, the dark counts of single-photon detectors will rise due to radiation exposure in orbit.

The current platform for the QEYSSat mission proposal is based on a microsatellite, to be located in a low Earth orbit (LEO) at an altitude of approximately 600 km. The payload would have an optical receiver with 40 cm aperture as the main optics (Figure 2). In order to show the viability of this mission concept, we have conducted several theoretical and experimental studies including a comprehensive link performance analysis, QKD experiments over high transmission losses and over a rapidly fluctuating channel.

We are currently working on the main technical challenges, which are to advance existing quantum devices to make them suitable for the space environment. The QEYSSat payload will include the capability to analyze and detect single optical photons with high efficiency and accuracy, and is aimed for a micro-satellite platform. In addition, we have considered the feasibility of nano-satellites, which could serve as an interesting technology demonstrator mission. The underlying principle of such payloads is that all arriving photon are analyzed in a polarization analyzer and detected in single-photon detectors. Onboard data acquisition will register all detection events and record their time-stamps to sub-nanosecond precision, which will be processed at a later time on the ground. We are leading a project with industry partners and the CSA to build and test a compact prototype for the main elements of the quantum key distribution receiver (QKDR) that would be compatible with a microsatellite-class platform.

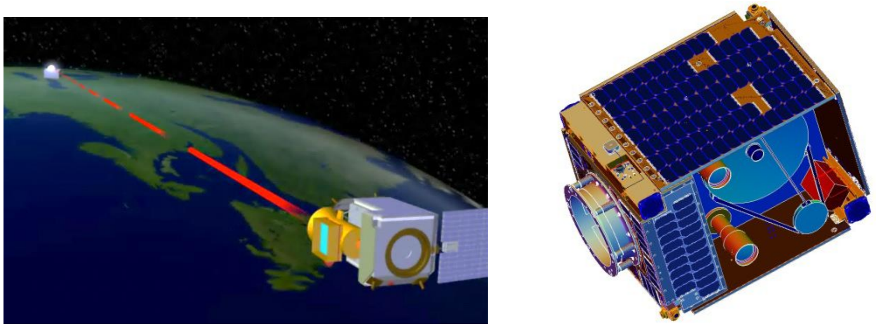

Figure 2: Left: Artist's rendering of a quantum communications link between a ground station and the satellite. Right: CAD drawing of the proposed QEYSSat spacecraft.

ACKNOWLEDGMENTS

This work is currently supported by the Canadian Space Agency (CSA), FedDev Ontario, NSERC, CIFAR, CFI Innovation Fund, Ontario Government MEDI ORF and ERA. An initial quantum microsatellite mission feasibility study had been funded by Defense Research and Development Canada (DRDC).

REFERENCES

[1] J. P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Huebel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. "A comprehensive design and performance analysis of low earth orbit satellite quantum communication." NEW JOURNAL OF PHYSICS, 15:023006, (2013).

[2] T. Jennewein and B. Higgins. The quantum space race. PHYSICS WORLD, 26(3):52–56, (2013).