# Astronaut Development and Deployment of a Secure Quantum Space Channel Prototype at the Pacific International Space Center for Exploration Systems

PISCES
Pacific International Space Center for Exploration Systems

# Astronaut Development and Deployment of a Secure Quantum Space Channel Prototype at the Pacific International Space Center for Exploration Systems

**Christopher Altman** (PISCES, University of Hawai'i), **Colin Williams** (NASA JPL, Caltech), **Rupert Ursin** (University of Vienna, Deputy Director, IQOQI, Austrian Academy of Sciences), **Paolo Villoresi** (University of Padova, Italy), **Vikram Sharma** (Quintessence Labs)

## Introduction

We propose a fundamentally new quantum communication system based on continuous-variable ***quantum teleportation*** that will provide space-based NASA assets with *unconditional information security*. All command-and-control inputs to spacecraft sent over our network will be guaranteed to be impossible to spoof by any US adversary, protected by the fundamental laws of physics, whereas there is currently no security proof for conventional secure communication such as SSL, RSA, *et al*. This type of absolute security is even guaranteed if the encrypted traffic must pass over insecure and public networks not under NASA, or even US, control. This capability will provide NASA with a ***permanent solution*** for its secure communication needs and is directly responsive to requirements for *unconditional information security* as referenced in the NASA Roadmap.

*Fig. 1. Optical communications equipment used to demonstrate quantum communications over 144km between La Palma and Tenerife.*

*Fig. 2. Astronauts field test next-generation extravehicular activity (EVA) spacesuits on analogue lunar surface terrain at PISCES atop the Mauna Kea volcano on the Big Island of Hawaii.*

Our visionary approach brings together the expertise of the two leading European groups involved in the world's-first demonstration of entangled quantum communications over a 144km free-space optical path, with the quantum and optical communications expertise of NASA JPL, the continuous-variable quantum communications expertise of Quintessence Labs, and the lunar and astronaut training facilities at the **Pacific International Space Center for Exploration Systems** (**PISCES**) on the summit of Mauna Kea, an active volcano on the Big Island of Hawai'i. Consequently, we offer the best global team for developing a free-space continuous-variable quantum communications prototype and demonstrating the feasibility for it to be set up and calibrated by NASA-trained astronauts conducting an analogue lunar training mission on the same terrain used to train Apollo 11 astronauts Neil Armstrong and Buzz Aldrin, echoing the famous placement of the lunar retroreflectors by the Apollo astronauts.

NASA is moving to optical communications for higher bandwidth channels. The security of those channels is based on standard public key infrastructure (PKI). As PKI is only *conditionally* secure, it can in principle be compromised with sufficient computing power. This exposes NASA's space assets – and astronauts – to potential harm if an adversary inserts damaging control inputs into communications used for command-and-control of space assets. We propose a functional system that an astronaut can set up to demonstrate the feasibility of deploying a secure quantum communications network between the Earth, the Moon, Mars, and deep space missions based on the use of continuous-variable quantum communications. This type of communications is ideally suited to integration into conventional NASA optical communications as it relies upon similar types of lasers and optical elements.

## Potential Impact

Our system dramatically surpasses the state-of-the-art in secure communications in two significant ways. First, whereas current information security relies upon public key cryptography, in which the security of the system rests on the unproven presumption that certain mathematical problems – such as factoring large composite integers or computing discrete logarithms – are intractable, the security of our quantum technique rests upon physical laws that cannot be circumvented. Secondly, whereas NASA and all other government agencies must periodically upgrade the security of their systems by using longer and longer cryptographic keys to keep one step ahead of those wishing to hack the communications channel, our proposed solution is derived from the known laws of fundamental physics, and is thus impervious to these kinds of attacks.

PISCES
Pacific International Space Center for Exploration Systems

## Study

***In Phase I**, we aim to achieve the following objectives:*

- Design the optical couplers between fiber-based continuous-variable quantum key distribution (CV-QKD) equipment and a free-space quantum communications channel between the Big Island and the Haleakalā observatory on Maui.
- At the High-Altitude Observatory Site in Science City, near the summit of Haleakalā volcano on the island of Maui, the Air Force Office of Scientific Research (AFOSR) operates the Maui Space Surveillance Complex (MSSC), part of the Air Force Maui Optical and Supercomputing Site (AMOS).
- The MSSC provides the 3.67 m (144 in) Advanced Electro-Optical System Telescope (AEOS), the Maui Space Surveillance System (MSSS), and the Ground-based Electro-Optical Deep Space Surveillance (GEODSS).
- MSSS provides a number of optical assets including a 1.6 m (63 in) telescope, two 1.2 m (47 in) telescopes, a 0.8 m (31 in) beam tracker and a 0.6 m (24 in) laser beam director.
- Install optical transmitter and receiver telescopes over a free-space CV-QKD link between PISCES on Mauna Kea and MSSS on Haleakalā at varying levels of optical losses. Assess CV-QKD link budget and model expected key rate under realistic conditions.
- Install, calibrate, and demonstrate the CV-QKD equipment at the PISCES test site. This will verify the CV-QKD is working at altitude prior to conducting any free-space tests.
- Demonstrate launch and intercept of the keys generated by the CV-QKD equipment from transmitter telescope to receiver telescope.
- Demonstrate successful key exchange with cryptographic keys imprinted on phase and amplitude quadratures of a bright coherent laser beam at the test site.
- Field-test ***Tx*** and ***Rx*** setups over short-range optical free-space channel with experimental simulation of losses to demonstrate application of the technology to the domain and resolve feasibility of a deep space secure quantum channel for secure quantum communications and teleportation.
- At the end of ***Phase I***, principal research team members comprised of spaceflight-ready NASA-trained astronauts and astronaut instructors will have successfully demonstrated the first *de novo* setup, alignment, calibration and testing of a secure quantum communications network.
- Our demonstration takes place at the same analogue lunar testing location historically chosen to train the NASA Apollo astronauts for the first manned missions to the Moon.

*Fig. 3. Retroreflector placed on the Moon by the Apollo astronauts.*

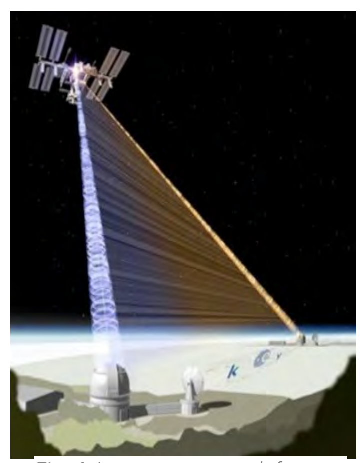


*Fig. 4. Long-term research for secure space communications.*

# Astronaut Development and Deployment of a Secure Quantum Space Channel Prototype at the Pacific International Space Center for Exploration Systems

**Quantum entanglement** holds the potential to revolutionize NASA's mission and effectiveness. Guaranteed secure communications are critical to NASA assets and to the lives of NASA astronauts. We propose a fundamentally new quantum-based communication system based on continuous variable quantum communications to establish a secure ***quantum teleportation*** link that will provide unconditional information security to NASA assets on the Moon, to Mars, to asteroids and deep space. Our proposal will demonstrate the feasibility of this system in an analog lunar environment, bringing quantum communications to the next-generation NASA manned spaceflight program. The capacity will provide NASA a permanent solution to its secure communication needs, and is directly responsive to the stated need for unconditional information security referenced in the NASA Communication and Navigation Systems Technology Roadmap.

Our visionary approach brings together the expertise of the two leading European groups involved in the first-ever demonstration of entangled quantum communications over a 144 km free-space optical path, with the quantum and optical communications expertise of NASA JPL, the continuous variable quantum communications expertise of Quintessence Labs, the lunar and astronaut training facilities at the Pacific International Space Center for Exploration Systems on Hawai'i, and the expertise of an elite cadre of NASA-trained astronauts selected and trained by NASA astronauts and astronaut instructors to create the world's first commercial astronaut corps. Consequently, we offer the best global team for developing the first-ever free-space continuous variable communications prototype while demonstrating the feasibility for it to be set up and calibrated by an astronaut on analogue lunar terrain, echoing the famous placement of lunar retroreflectors by the Apollo astronauts.

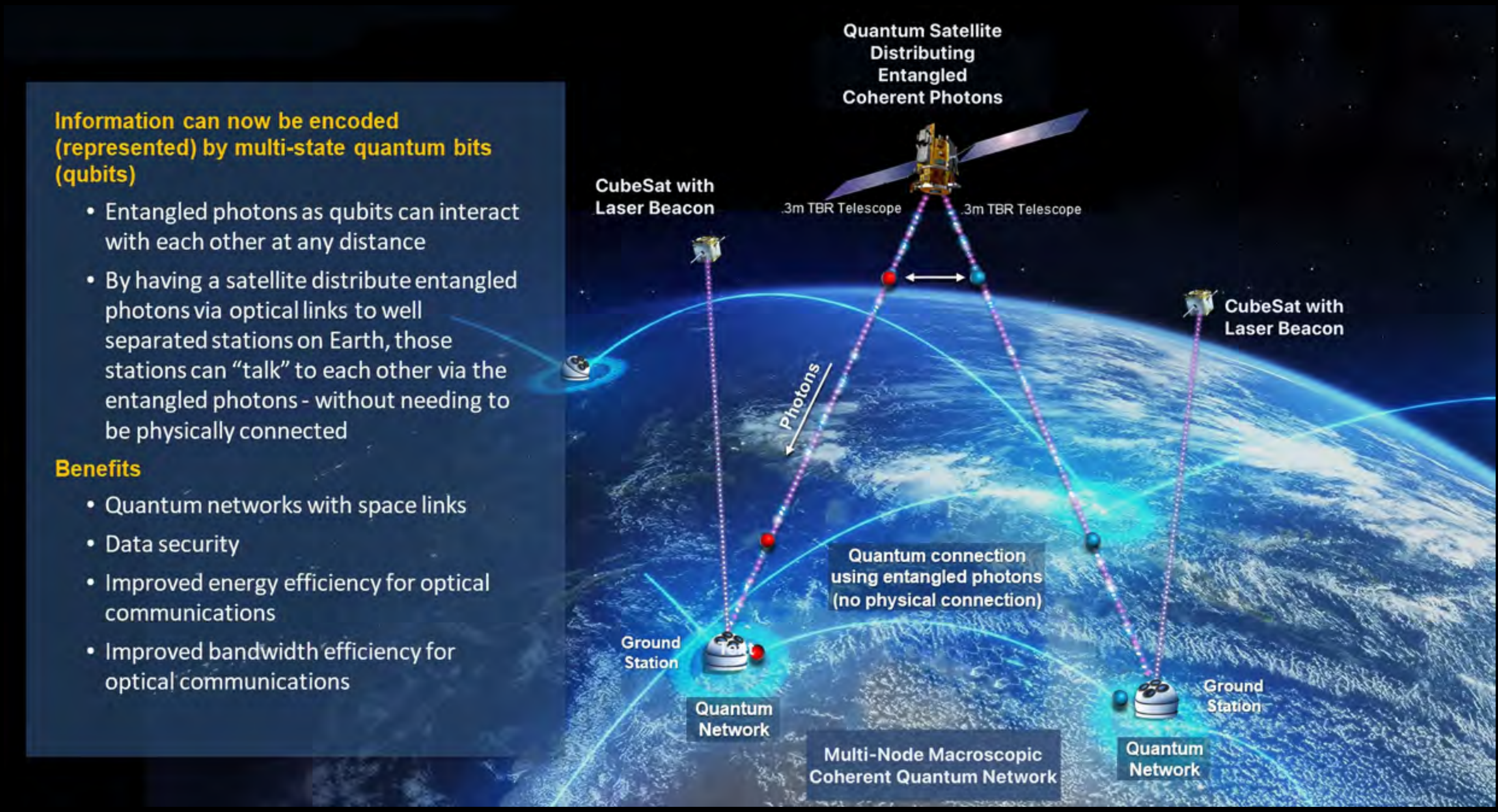
NASA is already moving towards optical communications for higher bandwidth channels. Currently the security of those channels is based upon standard public key infrastructure (*PKI*). As PKI is only *conditionally* secure it can, in principle *and in practice* be compromised with sufficient computing power. This exposes NASA's space assets and astronauts to potential harm if an adversary gains access and is able to insert damaging control inputs into communications commanding and controlling those assets. We propose a demonstration kit that an astronaut could set up to demonstrate the feasibility of deploying a ***secure quantum communications network*** between the Earth, the Moon, Mars, and deep space missions based on the use of continuous-variable quantum communications.

This type of entangled quantum communications is ideally suited to integration into conventional NASA optical communications as it relies upon similar types of lasers and optical elements. Hence, this concept represents a potential breakthrough in free-space quantum communications for NASA. The continuous-variable quantum communications system would be used to securely establish matching cryptographic keys over an (*potentially*) insecure channel. Thereafter, those keys could be used in any secure classical cryptographic system to guarantee authentication of command-and-control inputs sent to any NASA space asset, regardless of distance. ***Ultimately, this novel approach to communications will protect NASA assets and the lives of NASA astronauts***.

Project Summary from NASA/NIAC Phase I

# Astronaut Development and Deployment of a Secure Quantum Space Channel Prototype at the Pacific International Space Center for Exploration Systems

**Christopher Altman** (PISCES, University of Hawai'i), **Colin Williams** (NASA JPL, Caltech), **Rupert Ursin** (University of Vienna, Deputy Director, IQOQI, Austrian Academy of Sciences), **Paolo Villoresi** (University of Padova, Italy), **Vikram Sharma** (Quintessence Labs)



# REFERENCES


1. J. P. Dowling and G. J. Milburn, "Quantum Technology: the Second Quantum Revolution," *Philosophical Transactions of the Royal Society A*, Vol. **361**, No. 1809, 2003.

2. V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced Measurements: Beating the Standard Quantum Limit," *Science*, Vol. **306**, No. 5700, *pp*. 1330–1336, 2004.

3. N. Gisin and R. Thew, "Quantum Communication," *Nature Photon*ics, Vol. **1**, *pp*. 165–171, 2007.

4. R. P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, Vol. **21**, *pp*. 467–488, 1982.

5. W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside Quantum Repeaters," *IEEE Journal of Selected Topics in Quantum Electrons*, Vol. **21**, No. 3, 6400813, 2015.

6. K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, "Tools for Quantum Network Design," AVS *Quantum Science*, Vol. **3**, No. 1, 014101, Feb. 2021.

7. J. Preskill, "Quantum Computing in the NISQ Era and Beyond," *Quantum*, Vol. **2**, 79, 2018.

8. K. Nemoto, S. Devitt, and W. J. Munro, "Noise Management to Achieve Superiority in Quantum Information Systems," *Philosophical Transactions of the Royal Society A*, Vol. **375**, No. 2099, 20160236, 2017.

9. J. Kelly, "A Preview of Bristlecone, Google's New Quantum Processor," Google Quantum AI Lab, 2018.

10. F. Arute *et al*, "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, Vol. **574**, *pp*. 505–510, 2019.

11. H. S. Zhong, H. Wang, Y. H. Deng, M. C. Chen, L. C. Peng, Y. H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X. Y. Yang, W. J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N. L. Liu, C. Y. Lu, and J. W. Pan, "Quantum Computational Advantage Using Photons," *Science*, Vol. **370**, No. 6523, *pp*. 1460–1463, 2020.

12. M. Hanks, M. P. Estarellas, W. J. Munro, and K. Nemoto, "Effective Compression of Quantum Braided Circuits Aided by ZX-Calculus," *Physical Review X,* Vol. **10**, No. 4, 041030, 2020.

13. K. Nemoto, M. Trupke, S. J. Devitt, A. M. Stephens, B. Scharfenberger, K. Buczak, T. Nöbauer, M. S. Everitt, J. Schmiedmayer, and W. J. Munro, "Photonic Architecture for Scalable Quantum Information Processing in Diamond," *Physical Review* X, Vol. **4**, No. 3, 031022, 2014.

14. J. Sidhu, S.K. Joshi, M. Gundogan, T. Brougham, D. Lowndes L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone, P. Villoresi, A. Ling, T. Jennewein, M. Mohageg, J. Rarity, I. Fuentes, S. Pirandola, D.K.L. Oi, "Advances in space quantum communications," IET Quantum Communication, Institution of Engineering and Technology (IET)}, Vol **2**, no. 4*, pp*. 182-217, 2021.