Квантовое распределение ключей через атмосферные каналы связи

Сергей Кулик

ЦЕНТР КВАНТОВЫХ ТЕХНОЛОГИЙ
МГУ имени М.В. Ломоносова

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени
М.В.Ломоносова

Центр Квантовых Технологий

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

РусКрипто, 25 марта 2021

Центр Квантовых Технологий

КВАНТОВАЯ КОММУНИКАЦИЯ/СВЯЗЬ

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Волоконно-оптические Системы

Свободное пространство

Квантовые интерфейсы и память

ВЫВОД ЗАЩИТЫ ИНФОРМАЦИИ НА ПРИНЦИПИАЛЬНО ИНОЙ УРОВЕНЬ!

Квантовая коммуникация – это область знаний/техники о передаче квантовых состояний между удаленными объектами

Центр Квантовых Технологий

Основные направления мировых разработок

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

1. **Волоконно-оптические линии связи**
- шифрование квантовыми ключами данных, передаваемыми по магистральным линиям связи
- создание локальных защищенных сетей с электронным документооборотом
- создание крупномасштабных сетевых структур через доверенные узлы

2. Атмосферно-космические каналы связи
- распределение квантовых ключей между мобильными и стационарными объектами
- распределение ключей между низкоорбитальными спутниками и наземными объектами
- распределение ключей между низко- и высокоорбитальными спутниками
- создание глобальных квантовых сетей, охватывающих значительные территории

По всем направлениям работа ведется при поддержке
Фонда перспективных исследований,
НТИ (Центр квантовых технологий, Центр квантовых коммуникаций),
Министерства обороны РФ, ФСБ России, Министерства науки и высшего образования и др.,
РФФИ, РНФ, Фонд Бортника

Центр Квантовых Технологий

Квантовое распределение ключей через открытое пространство

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

1. Квантовое распределение ключей – демонстрационные эксперименты

2000-2001 Первые работы по распределению ключей на расстояния порядка 1 км
2007-2009 Рекорд дальности по распределению ключей и передаче запутанности (144 км)
2012 Распределение перепутанности и квантовая телепортация на 97 км

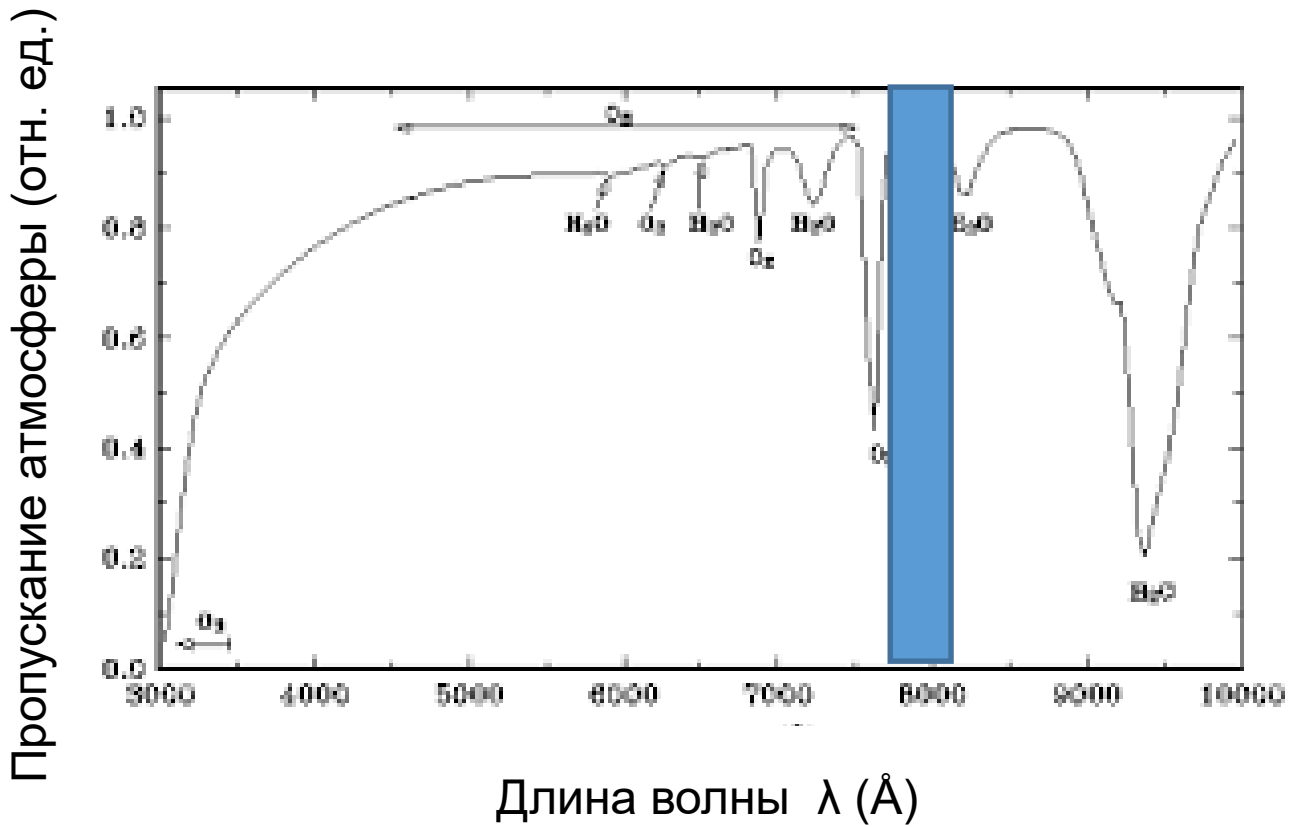
2. Квантовое распределение ключей на движущиеся объекты

2013 Квантовое распределение ключей на самолет
2015 Квантовое распределение ключей на движущийся автомобиль
2017 Распределение ключей между дронами

3. Спутниковые системы квантовых коммуникаций

2014 SOTA/SOCRATES optical space terminal (NICT, Japan)
2016 Источник пар фотонов на орбите (Сингапур); **Micius satellite (China)**
2017 Квантово-ограниченная передача с геостационара (Alphasat)
2020 Эксперимент по оптической связи «Эколинс» (Роскосмос)

Спектральное пропускание атмосферы



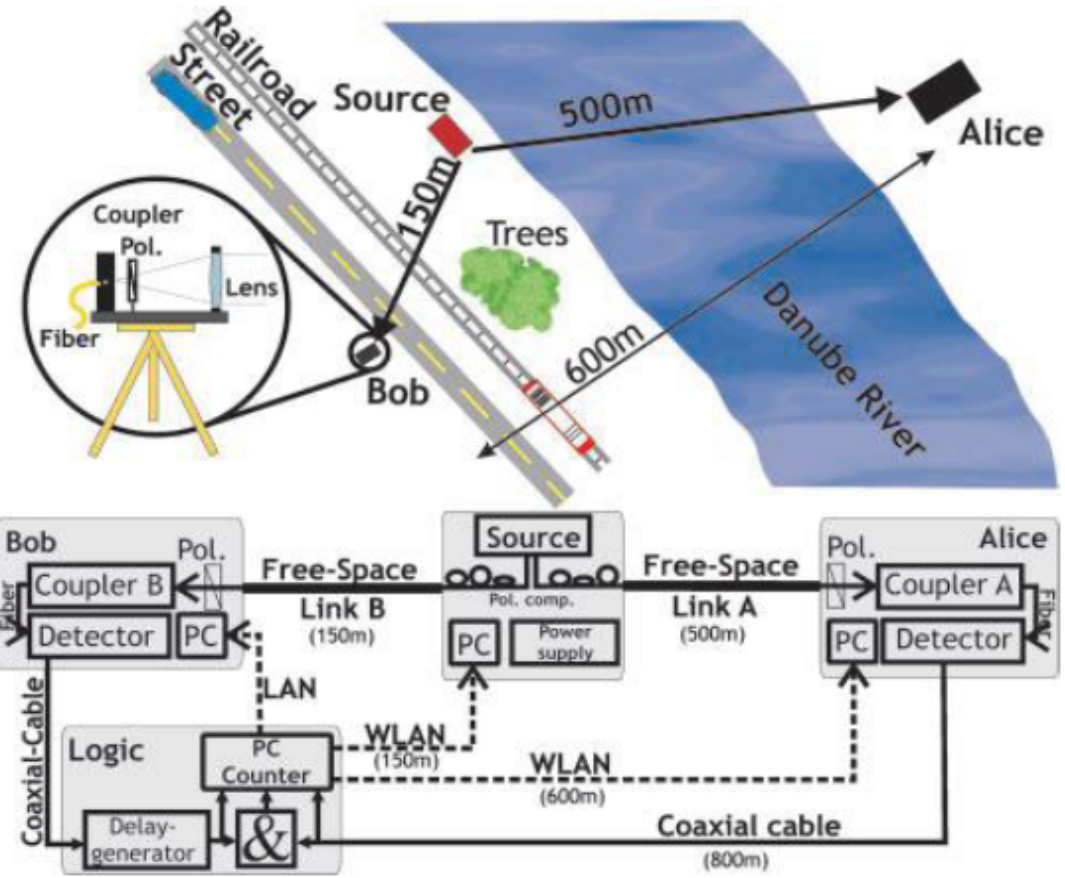
Компромисс между пропусканием и квантовой эффективностью однофотонного приемника

Центр Квантовых Технологий

РАСПРЕДЕЛЕНИЕ ПЕРЕПУТЫВАНИЯ НА БОЛЬШИЕ РАССТОЯНИЯ ЧЕРЕЗ СВОБОДНОЕ ПРОСТРАНСТВО

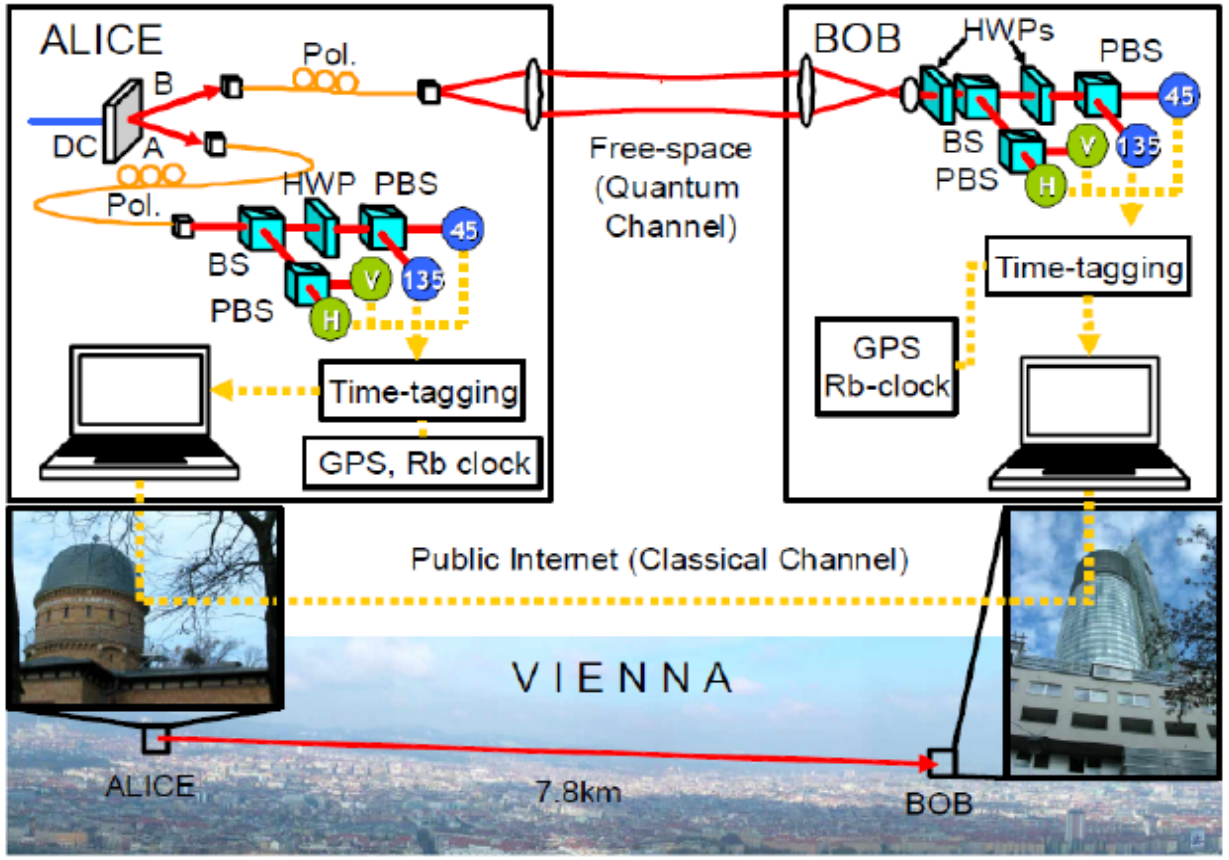
ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Over 600m



Experiment in Vienna, Austria, 2003

Over 7.8km



Experiment in Vienna, Austria, 2005

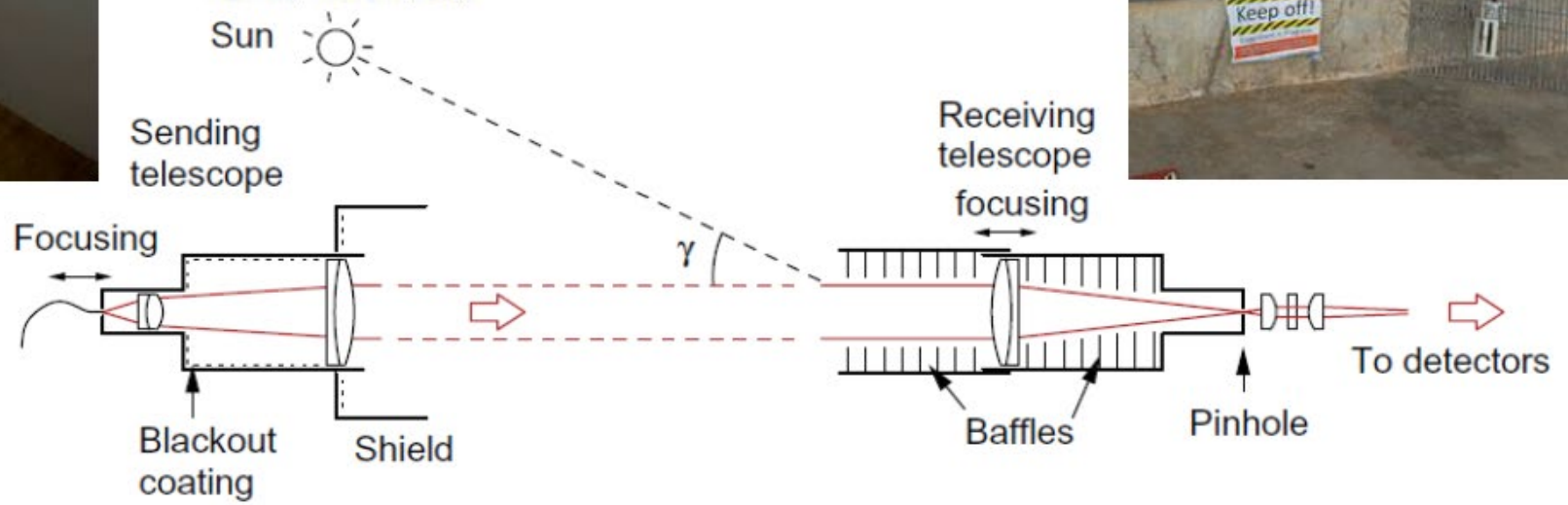
M. Aspelmeyer, et al. "Long-Distance Free-Space Distribution of Quantum Entanglement" Science 301, 621 (2003)
K.J. Resch at al. "Distributing entanglement and single photons through an intra-city, free-space quantum channel"

Центр Квантовых Технологий

КРК ПРИ ДНЕВНОМ ОСВЕЩЕНИИ

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

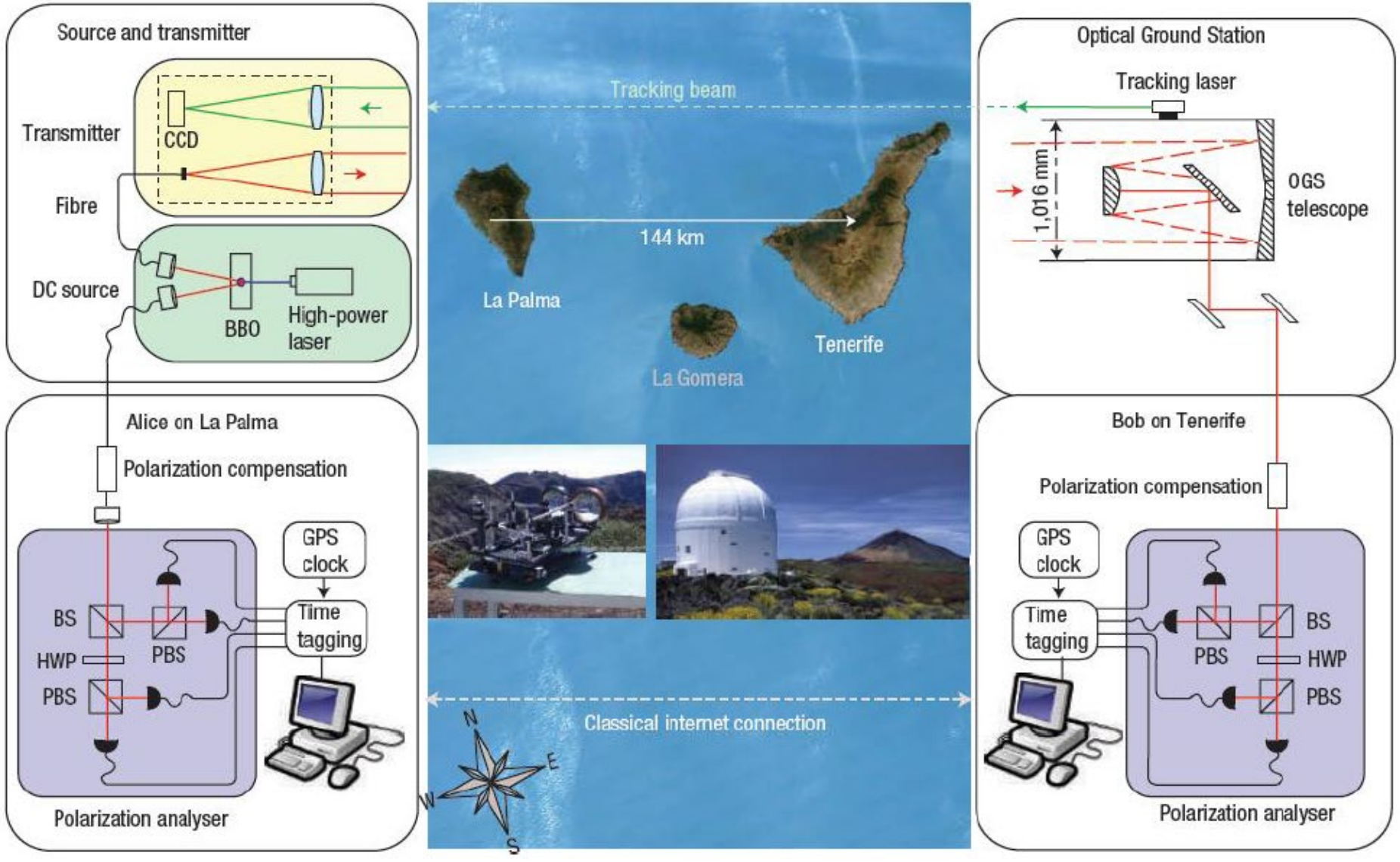
APL 89, 101122 (2006)



M.P. Peloso at al. "Daylight operation of a free space, entanglement-based quantum key distribution system" New Journal of Physics 11 (2009) 045007

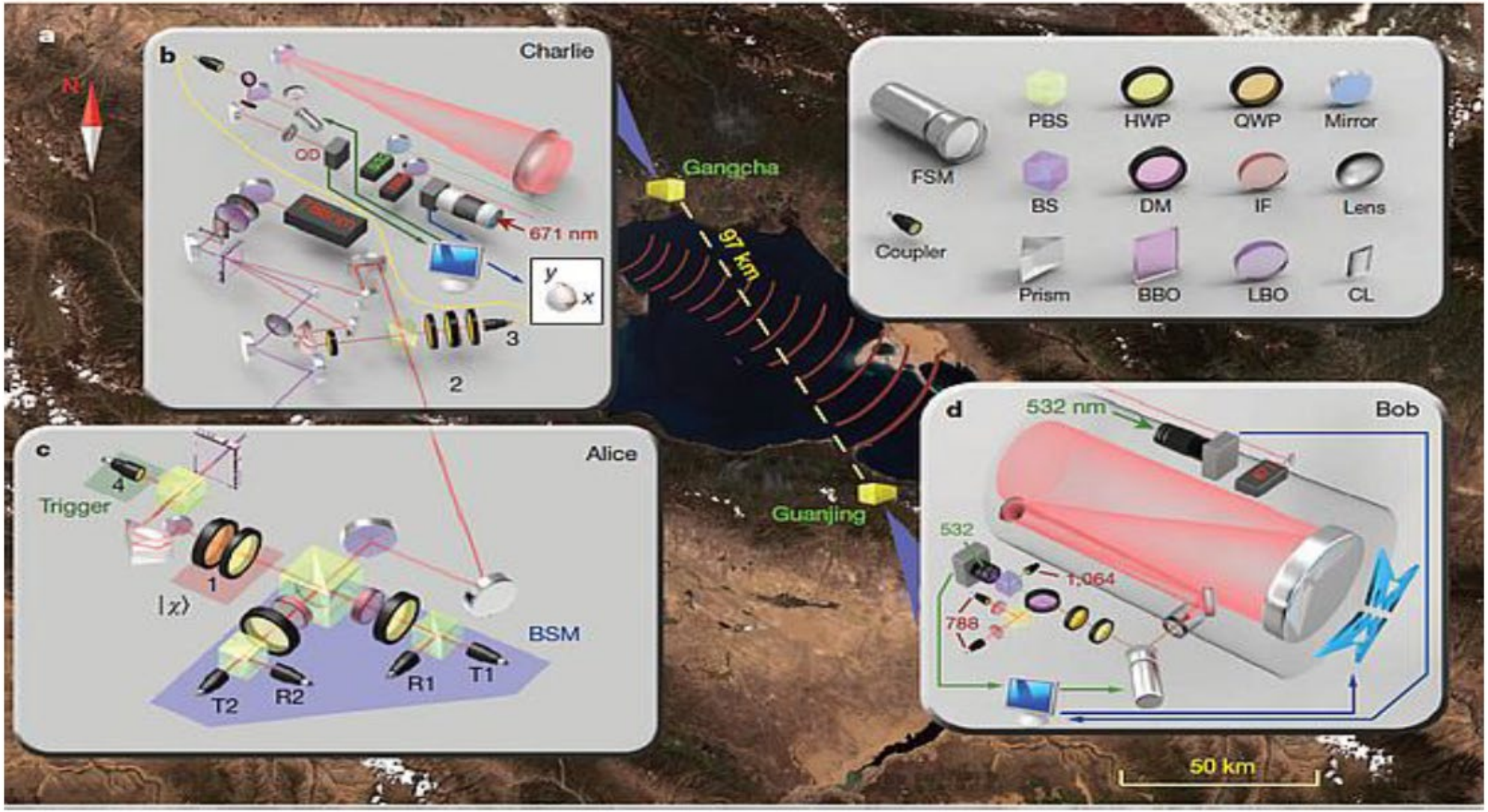
NUS National University of Singapore

КРК на расстоянии 144 км. Распределение запутывания между Канарскими островами



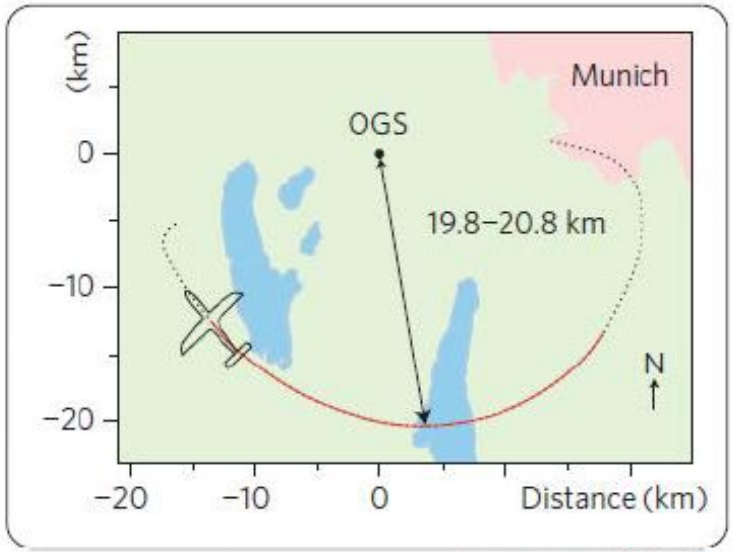
Ursin, R. et al. Entanglement-based quantum communication over 144 km. Nature Phys. 3, 481-486 (2007).

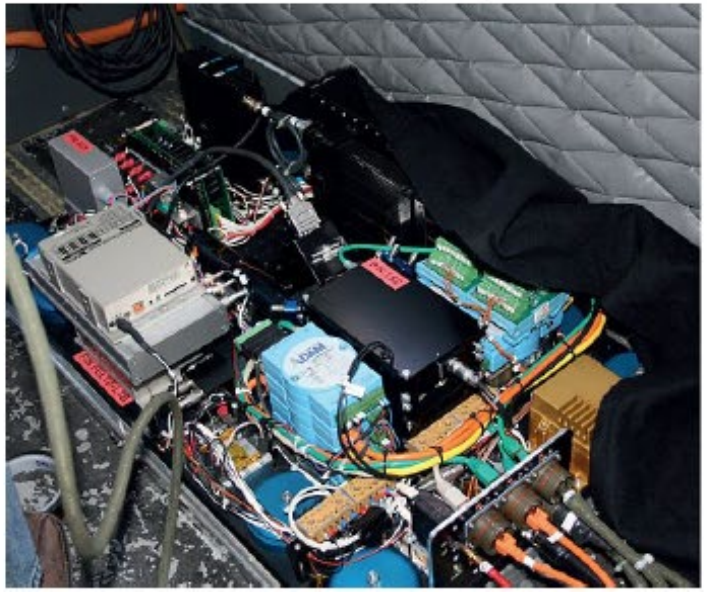
КВАНТОВАЯ ТЕЛЕПОРТАЦИЯ НА РАССТОЯНИИ 97 КМ

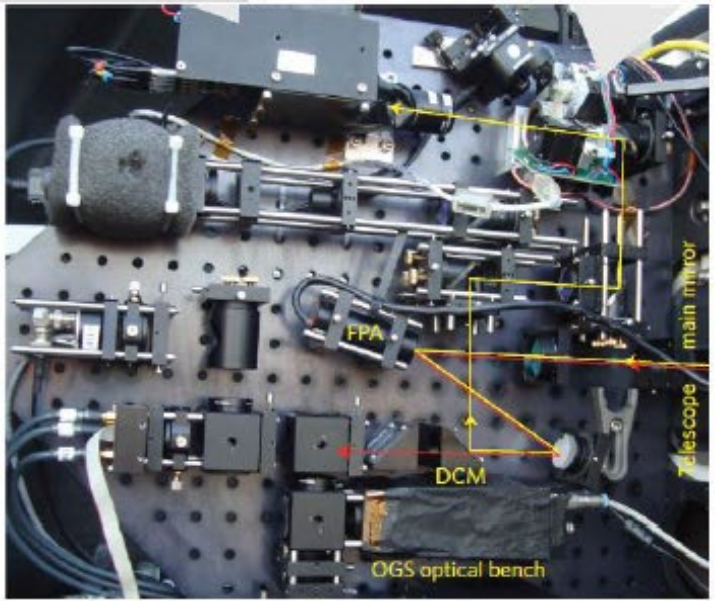


J. Yin, J.-G. Ren, H. Lu, at al. "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels", Nature, vol. 488, p.185. (2012) Китай

BB84 на ослабленных когерентных состояниях, поляризационное кодирование, дальность – 20 км, полная эффективность -38 дБ





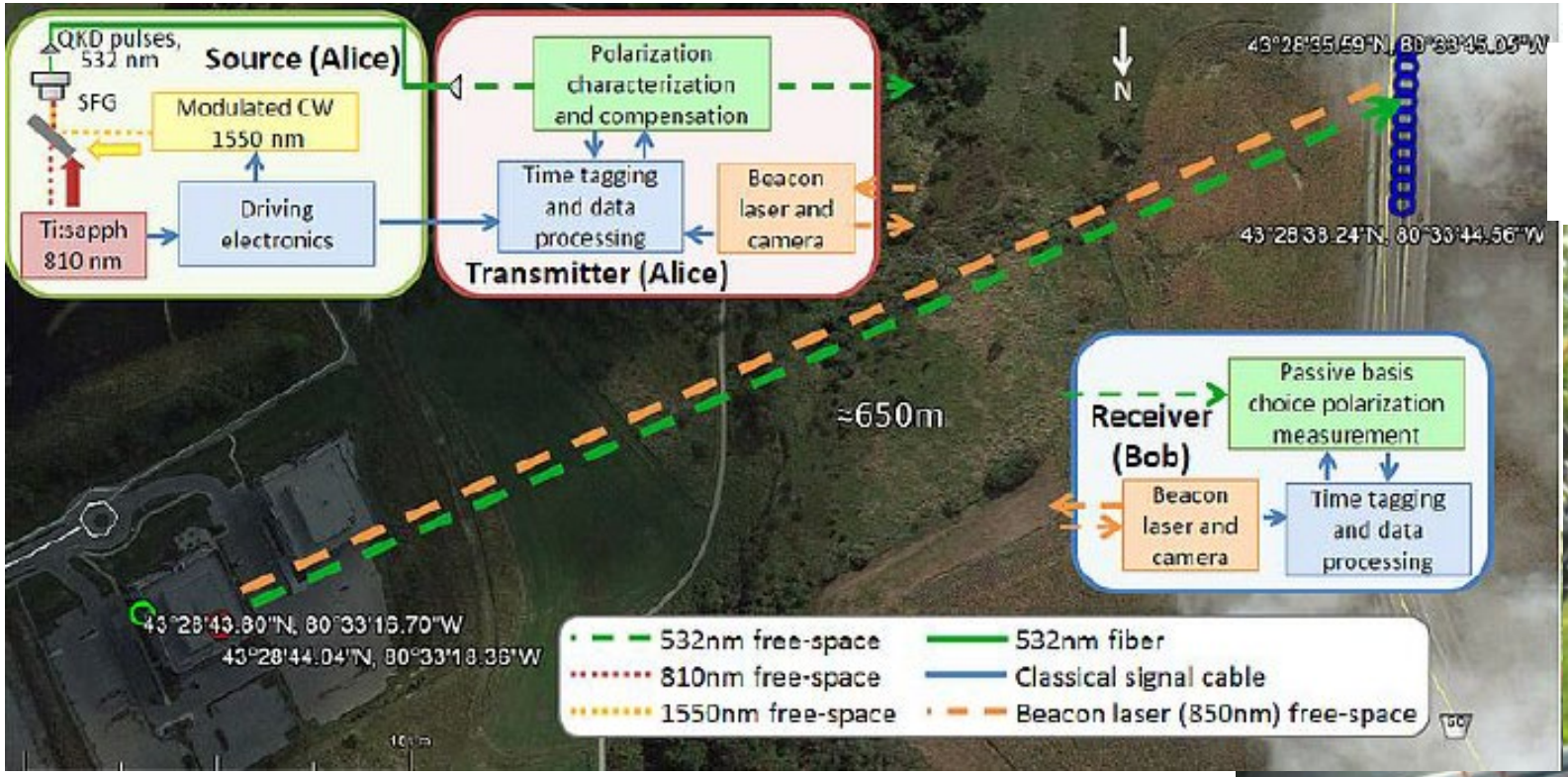


S. Nauerth at al. "Air-to-ground Quantum communication", Nature Photon. 2013

Центр Квантовых Технологий

КРК между стационарной станцией и движущимся автомобилем

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

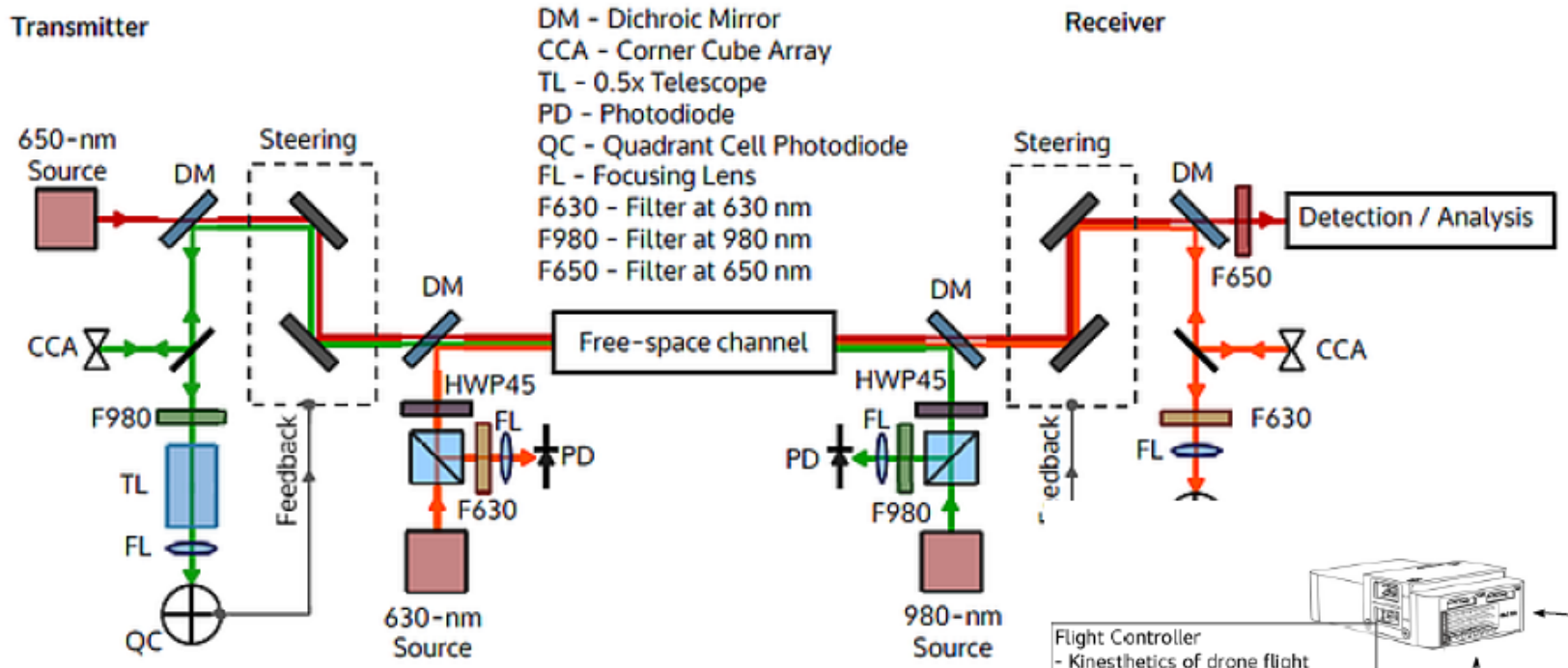


BB84 decoy-state

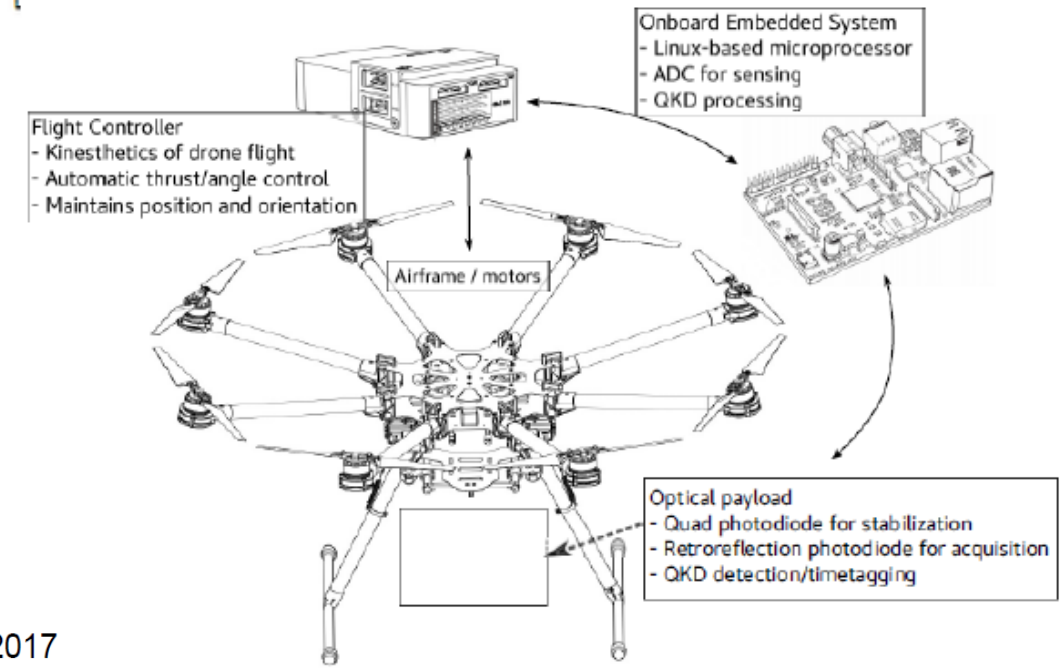
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

J.-P. Bourgoin, B. L. Higgins, N. Gigov, at al.
“**Free-space quantum key distribution to a moving receiver**”, Opt. Express v. 23, 33437 (2015)

КРК между стационарной станцией и ДРОНом



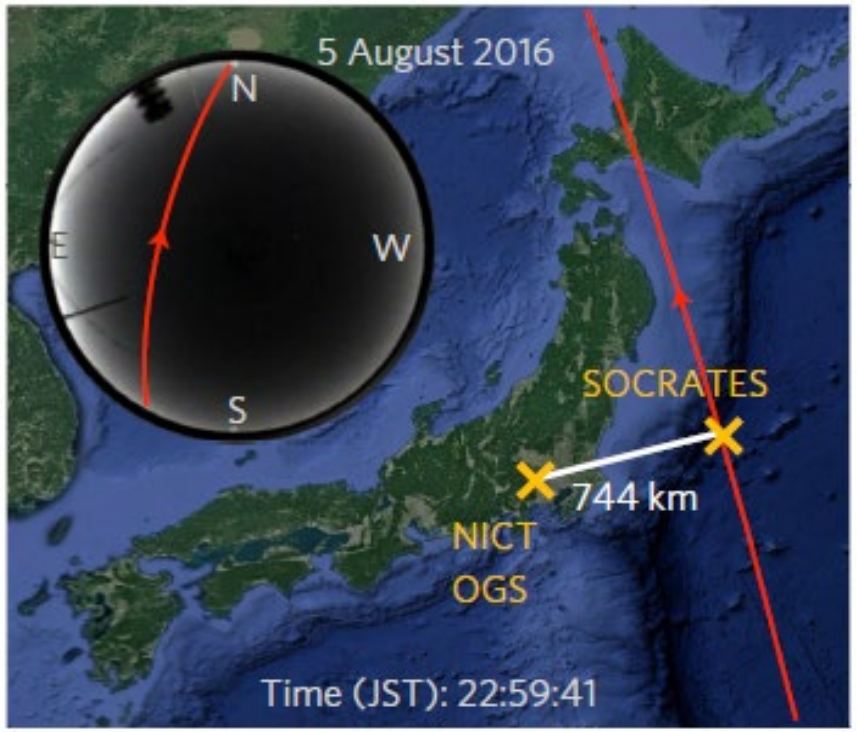
3-state protocol

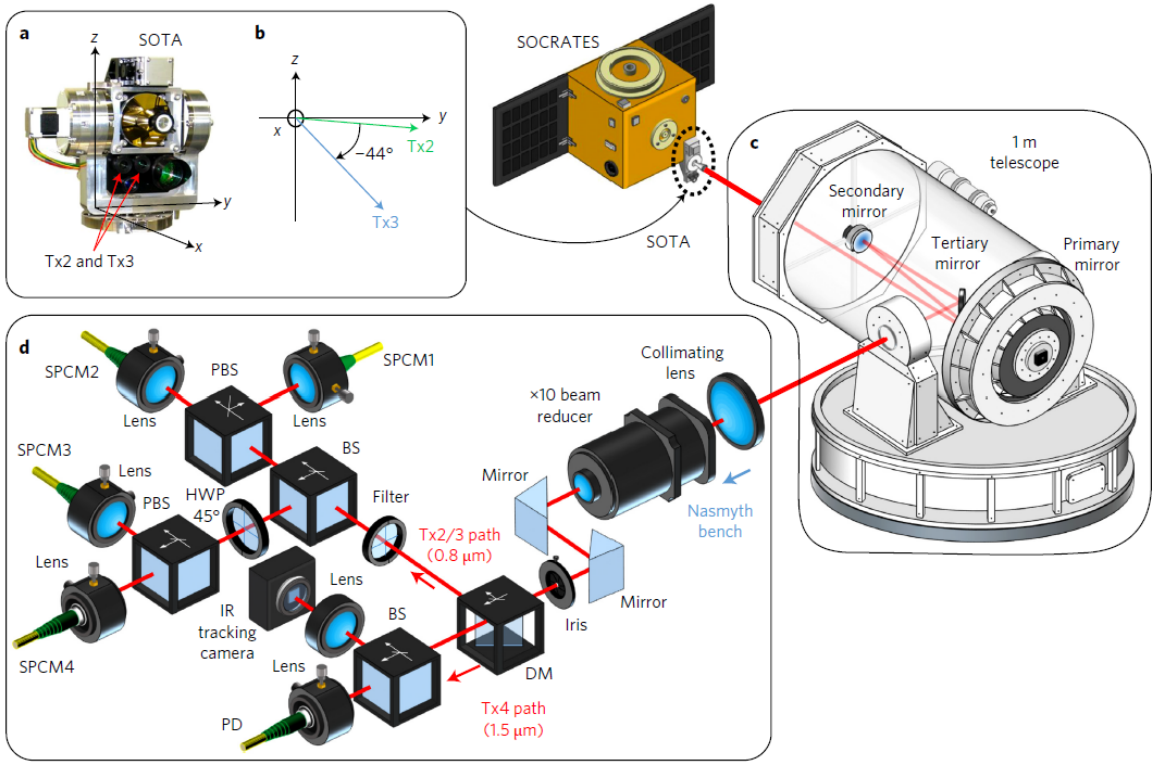


A. D. Hill, J. Chapman, K. Herndon, C. Chopp, D. J. Gauthier, Paul Kwiat, 2017

Квантовая спутниковая связь (2014)

2014 – SOTA/SOCRATES optical space terminal (NICT, Japan): микроспутник 50 кг.
Измерение поляризационных состояний, «квантово-ограниченная» передача данных на землю.
Передатчик на спутнике, прием наземным 1,5 м телескопом.



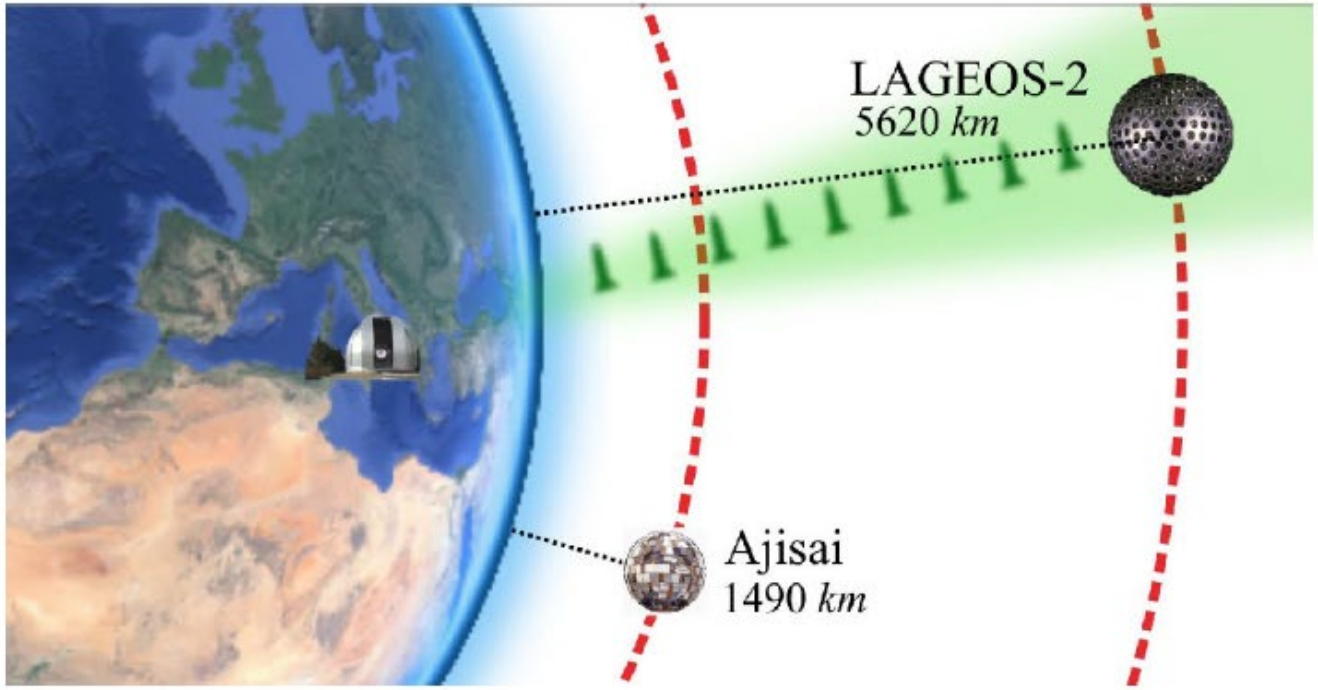


H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite" NATURE PHOTONICS, vol. 11, p. 502, 2017.

Single Photon exchange: from LEO to MEO

Серия экспериментов группы П.Виллорези

- **Эффективное (по наклону) расстояние 7000 км;**
- **Длина волны 532 нм;**
- **Энергия 1.1nJ;**
- **Частота повторения 100 МГц;**
- **Длительность импульсов 100 пс;**
- **Диаметр зеркала 1.5 м;**
- **Детектор – ФЭУ Hamamatsu$**
- **Интерфильтр 3 нм;**
- **Паразитная засветка < 50Гц.**



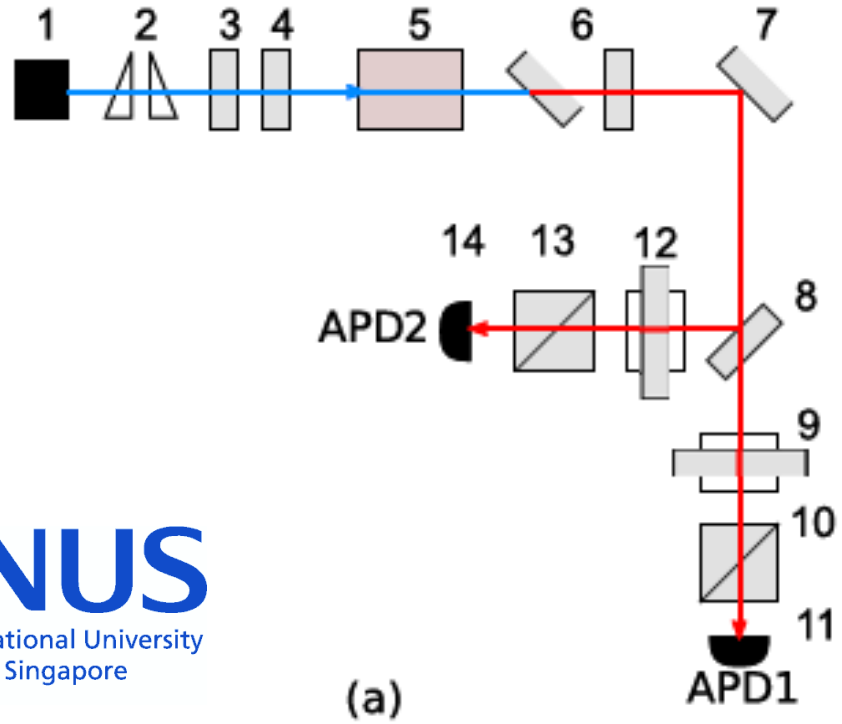
P. Villoresi et al., *Experimental verification of the feasibility of a quantum channel between space and Earth*," New J. Phys. **10** 033038, 2008.
D. Dequal et al. *Experimental single photon exchange along a space link of 7000 km*, PRA Rapid Comm **93** 010301, 2016.

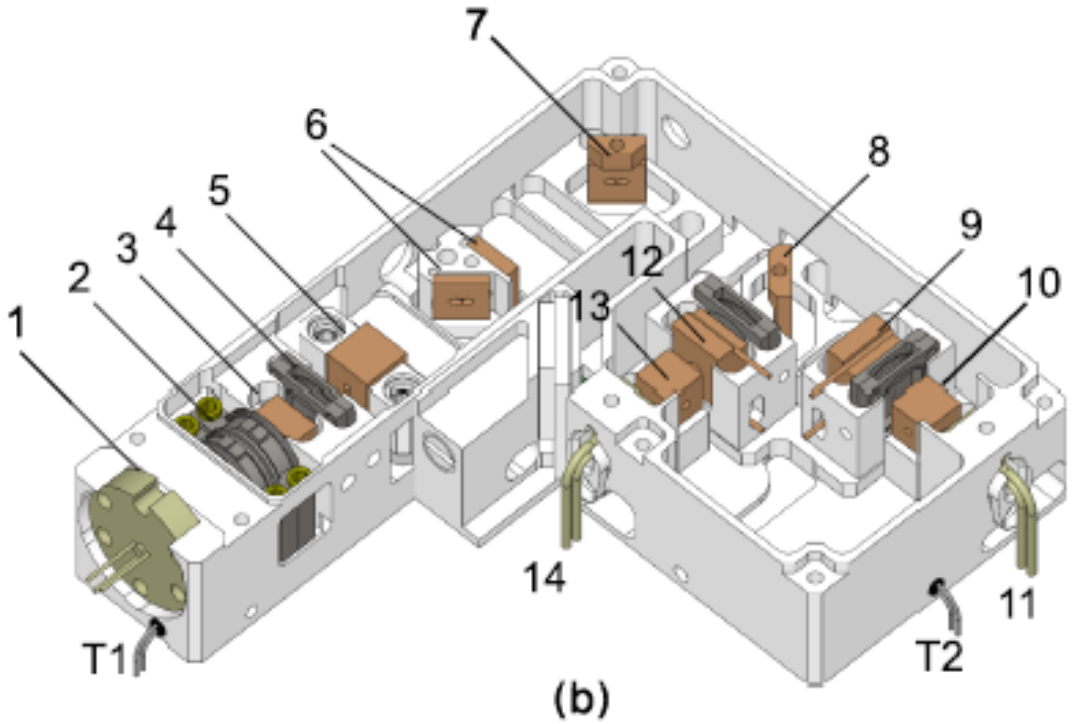
Центр Квантовых Технологий

Источник пар фотонов на орбите (2016)

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Первая попытка не удалась – взорвалась ракета-носитель, но источник в итоге остался цел.
Вторая попытка успешная. Режим генерации пар: невырожденный коллинеарный синхронизм типа I.





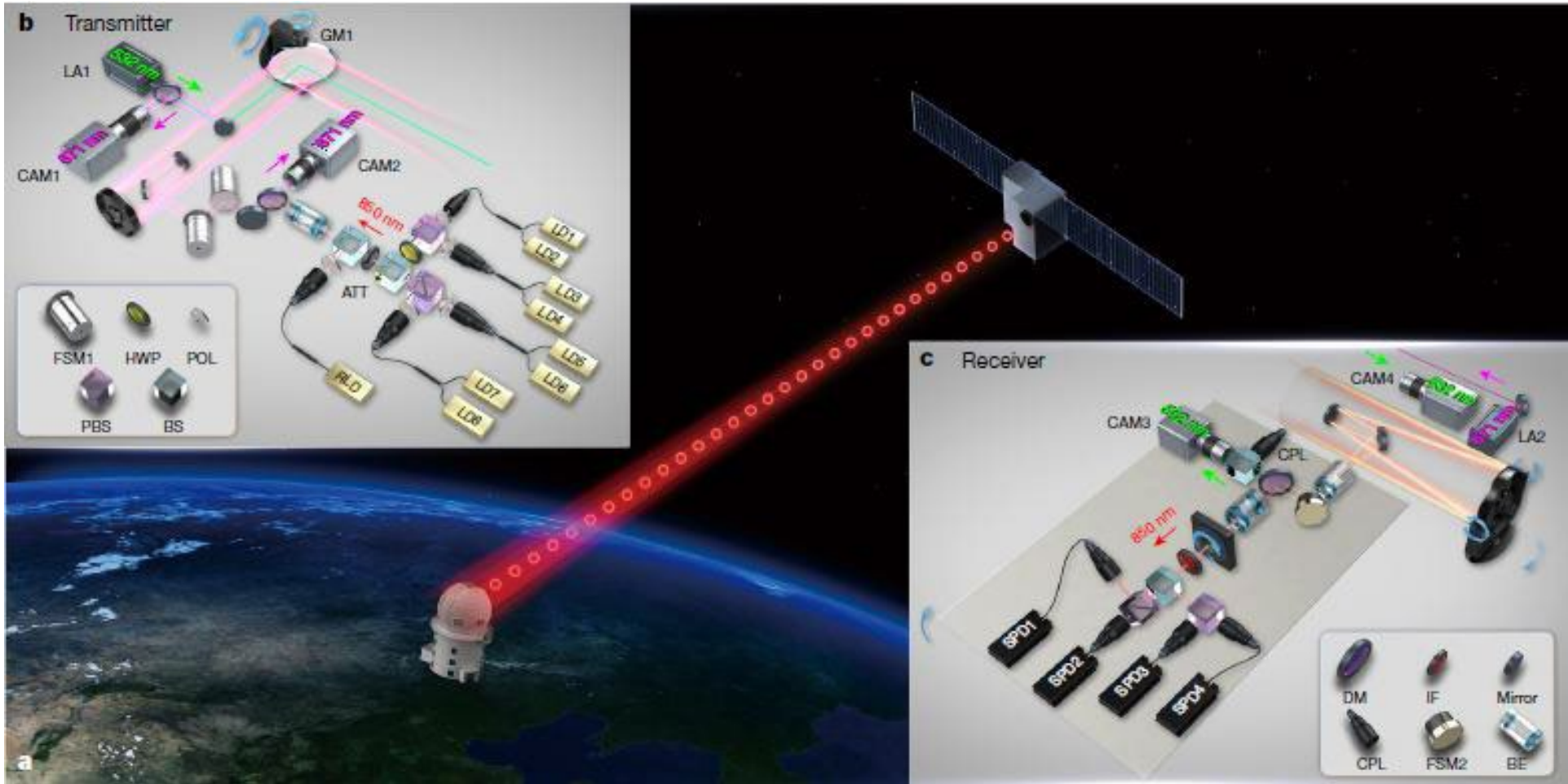
NUS National University of Singapore

Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel KL Oi, Alexander Ling"Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite", PHYSICAL REVIEW APPLIED 5, 054022 (2016).

Спутник Мисиус, Мо-цзы (Micius, China) 2016

Источник пар фотонов на борту (KTP, 810 нм); Два передающих телескопа (30 см и 18 см)
Наземные станции: (**два телескопа 1 м, и 1.8 м**)

Основные результаты:
2017: Распределение запутанных фотонов на 1200 км
2017: Квантовое распределение ключей со спутника на землю
2018: Спутник как доверенный узел: распределение ключей на 7800 км

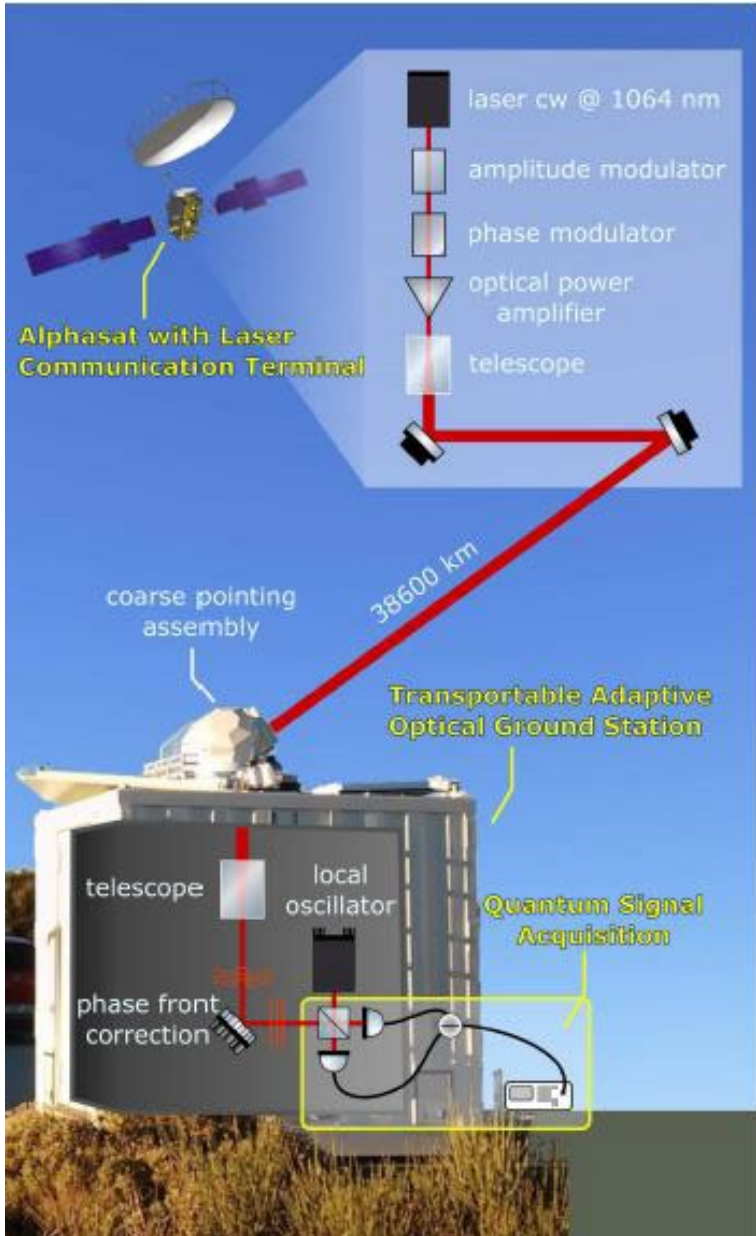


Центр Квантовых Технологий

Квантово-ограниченная передача с геостационарного спутника (Alphasat), 2017

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Alphasat (Inmarsat-4A F4)
дальность передачи - 38 600 км
Приемная апертура на земле - 27 см
Полные потери - 85 дБ
Длина волны - 1064 нм
Скорость передачи данных - 2.8 Гбит/сек
Бинарная фазовая модуляция



K. Günthner "Quantum-limited measurements of optical signals from a geostationary satellite", Optica, Vol. 4, No. 6, p.611, 2017.

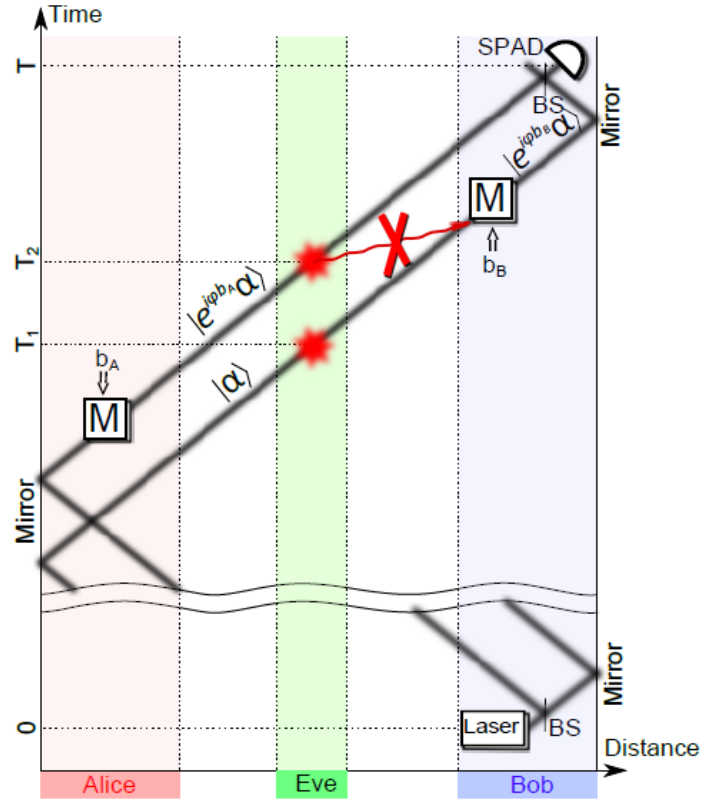
Центр Квантовых Технологий

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Квантовая коммуникация при произвольных потерях

Для всех известных протоколов требуется знать потери в канале *a priori.*

Принципиальный вопрос.
Существуют ли протоколы гарантирующие секретность ключей при любых потерях (заранее неизвестных и меняющихся в течение работы протокола) и неоднофотонном источнике?



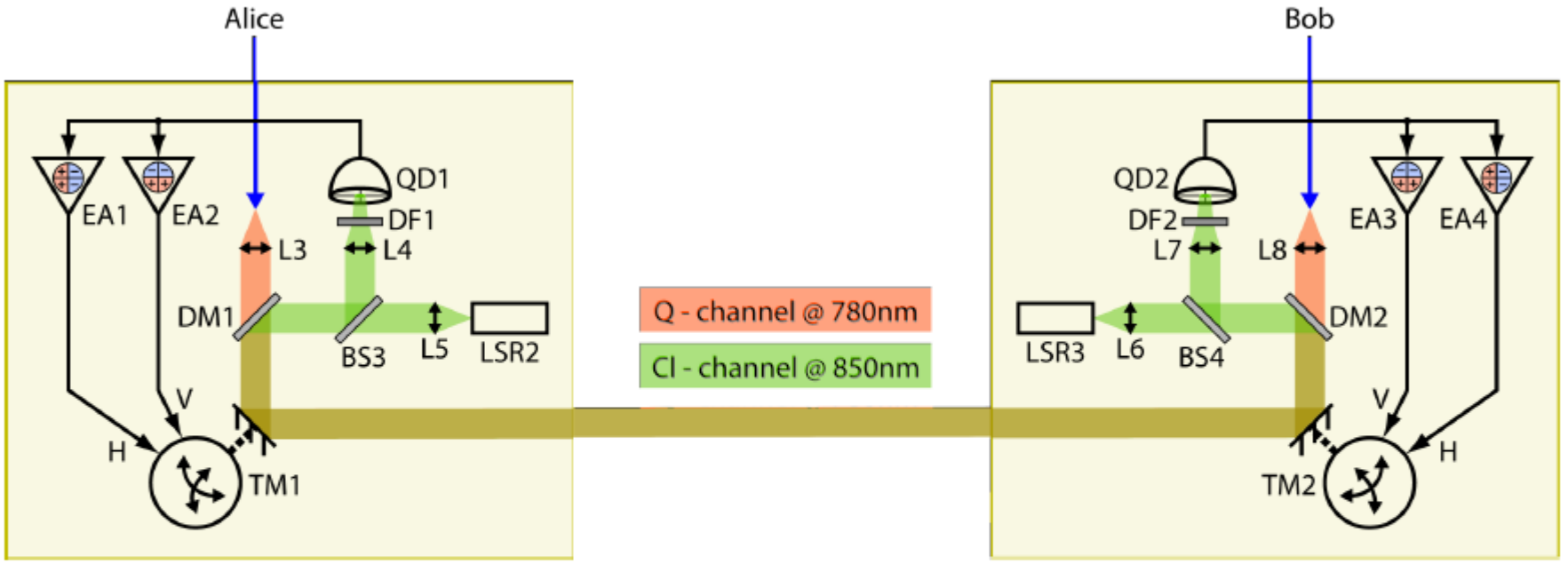
Фундаментальных ограничений только квантовой механики на измеримость квантовых состояний недостаточно.

Решение: Релятивистская квантовая криптография (проект ФПИ «ГАМАК»)

I V Radchenko, K S Kravtsov, S P Kulik and S N Molotkov, "Relativistic quantum cryptography", Laser Phys. Lett., vol. 11, no. 6, 065203 (2014).

Практическое использование

Схема системы трекинга



BS3, BS4 — светоделители,
DF1, DF2 — матовые пластинки,
DM1, DM2 — дихроичные зеркала,
EA1 … EA4 — усилители ошибки,

L3 … L8 — линзы,
LSR2, LSR3 — полупроводниковые лазеры,
QD1, QD2 — 4-секционные фотодетекторы,
TM1, TM2 — поворотные зеркала

MSU Quantum Technologies Center

КВАНТОВАЯ КОСМИЧЕСКАЯ СВЯЗЬ: ПРОЕКТЫ РФ

1. Долгосрочная программа научно-прикладных исследований и экспериментов, планируемых на РКС МКС до 2024 года –шифр «ЭКОЛИНС» (Роскосмос). Выведение на орбиту в 2024 г.

Цель выполнения СЧ ОКР – создание модуля передатчика поляризационных квантовых состояний для экспериментальной демонстрации возможности квантового распределения ключей и шифрования данных через космические аппараты.

Исполнители — ФГУП «РФЯЦ- ВНИИЭФ», Центр квантовых технологий МГУ и др.

2. Разработка приемного модуля системы квантового распределения ключей (КРК) по каналам «спутник-Земля».

Цель – создание модуля наземного терминала для обеспечения квантового распределения ключей и шифрования данных через космические аппараты.

Исполнители – АО Мостком, г. Рязань, Qrate, Центр квантовых технологий МГУ, РФЯЦ и др.

20

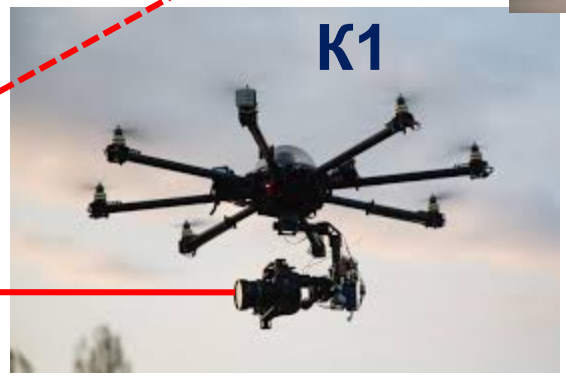
Центр Квантовых Технологий

Атмосферная квантовая криптография: КРК между стационарным Объектом и ДРОНом

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

2020 г. Распределение ключей между стационарным объектом (Ш) и мобильными летательными аппаратами (К1, К2, К3…) через мобильный летательный аппарат (К).

ПРОТОКОЛ: на перепутанных парах фотонов
Расстояние до 100 м (проект 2019-2020 гг.)

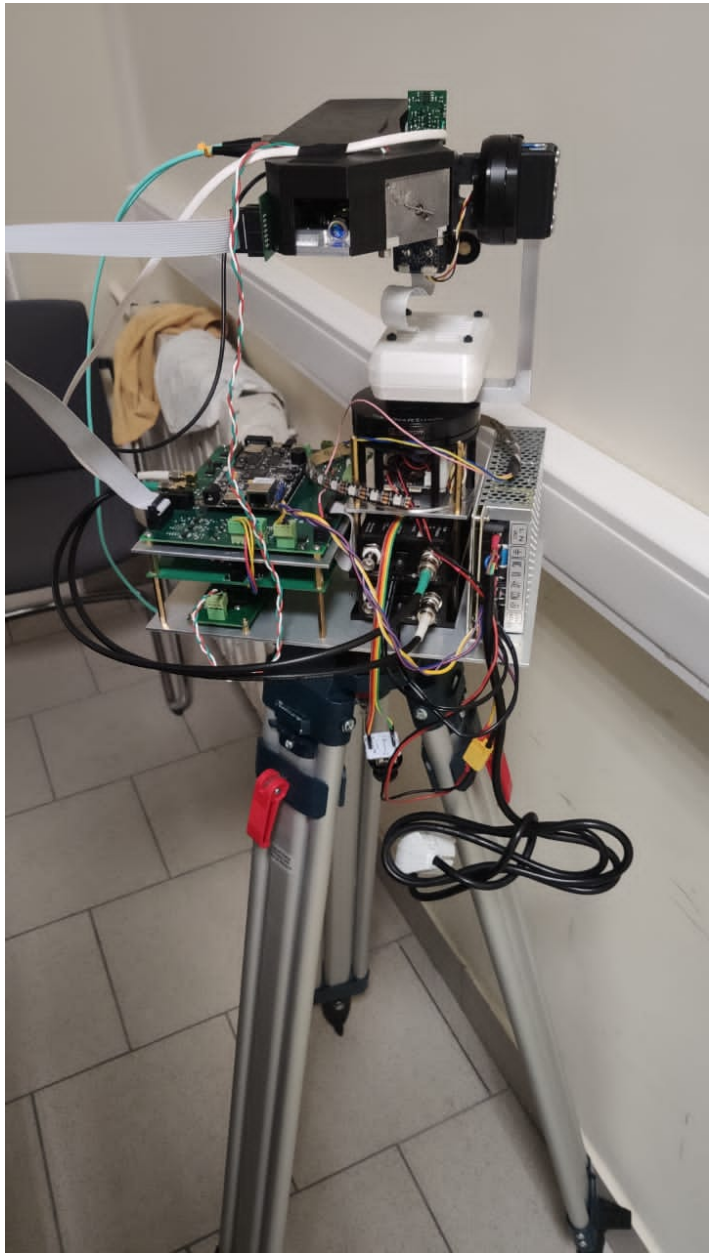


Центр Квантовых Технологий

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Атмосферная квантовая криптография: КРК между стационарным Объектом и ДРОНом

2020 г. Распределение ключей между стационарным объектом (Ш) и мобильными летательными аппаратами (К1, К2, К3…) через мобильный летательный аппарат (К).



Проблема расходимости пучка

- Для телескопа диаметром 0.5 м получаем T=0.48%, что ниже расчетного уровня в 1%.
- Для телескопа диаметром 0.75м получаем T=1.07%, что на грани допустимого.
- Для телескопа диаметром 1.0 м получаем T=1.9%, что уже может быть принято за соответствующую расчетным значениям величину*.

**данный расчет сильно идеализирован и не включает ни конечной ширины Гауссова пучка, ни ошибок в угле прицеливания, ни атмосферных искажений.*

Центр Квантовых Технологий

Команды:

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

QRATE
QUANTUM COMMUNICATIONS

Центр Квантовых Технологий

СМАРТС КВАНТТЕЛЕКОМ

ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КАЗАНСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК»

ВЫВОДЫ

1. Квантовое распределение ключей через атмосферные каналы – специфический случай:

- потери неизвестны;
- потери случайно меняются со временем;
- уровень потерь может превзойти критический – разрыв связи.

2. На сегодняшний день реализованы разные варианты систем КРК: стационар-стационар; стационар-мобил; мобил-мобил; стационар-НОС и др.

3. Перспектива их использования в массовых масштабах (коммерциализация) неочевидна: обсуждаются варианты ограниченного использования для специальных целей.

4. Построение глобальной защищенной сети с использованием технологии КРК возможно, но необходимо понять кому это нужно и для каких задач.

СПАСИБО ЗА ВНИМАНИЕ