ITMO UNIVERSITY

ПКС и защищенные квантовые коммуникации

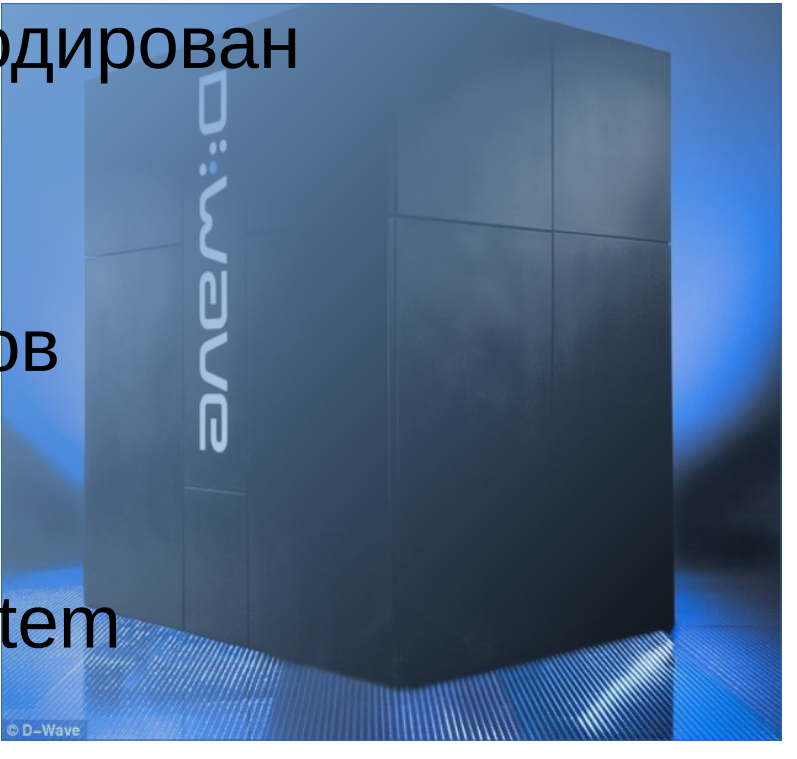
sadov@mail.ifmo.ru
Олег Садов

http://sdn.ifmo.ru/

ITMO UNIVERSITY

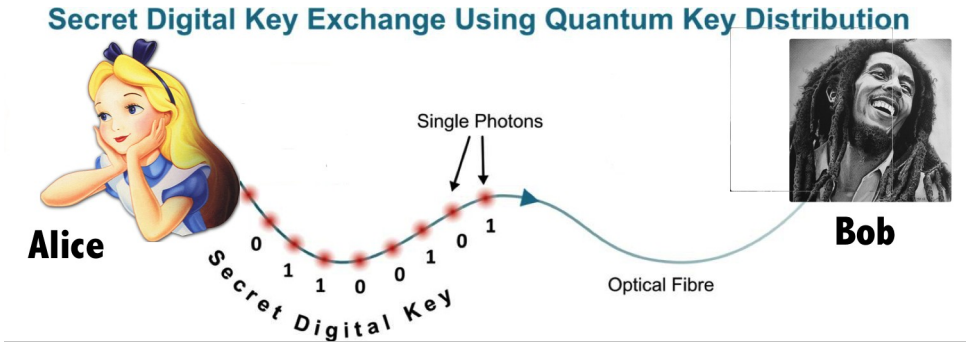
Проблемы существующих методов защиты информации

- Безопасность основана на том, что перехватчик не успеет расшифровать информацию, пока она актуальна
- В 2010 ключ RSA 768 bit был декодирован
- Увеличение длины ключей перегружает инфраструктуру
- Появление квантовых процессоров угрожает традиционным шифрам
- Sep 27, 2016 – D-Wave Systems Previews 2000-Qubit Quantum System



ITMO UNIVERSITY

Post-Quantum Cryptography



- NIST. Workshop on cybersecurity in a post-quantum world, 2015. http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm
- Erdem Alkim, Léo Ducas, Thomas Pöppelmann. Post-quantum key exchange – a new hope. https://eprint.iacr.org/2015/1092.pdf
- Amy Nordrum. Quantum Computer Comes Closer to Cracking RSA Encryption. 3 Mar 2016. http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment
- Matt Braithwaite. Experimenting with Post-Quantum Cryptography. July 7, 2016. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html
- Bruce R. Auburn. Quantum Encryption – A Means to Perfect Security? GSEC v.1.4b. https://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986

ITMO UNIVERSITY

Multinode quantum networks

QKD Networks:

1. SECOQC QKD network (below)
2. DARPA (USA)
3. SwissQuantum
4. Tokyo QKD
5. Battelle — First Commercial Quantum Key Distribution Protected Network (USA)
6. Quantum Experiments at Space Scale (QUESS) satellite (China)

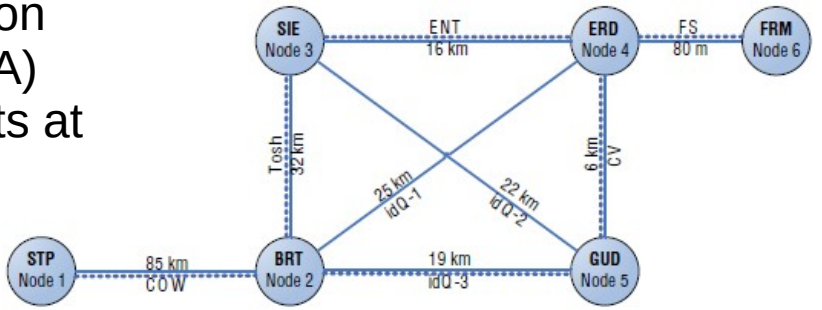


Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.

Eight node point-to-point network (Austria):

- idQuantique (3 devices)
- Toshiba Research
- GAP Optique
- University of Vienna
- Centre National de la Recherche Scientifique
- Ludwig Maximillians University (free space)

Mean distance **25 km**, bitrate **10 kbit/s**, maximum distance **80 km**

M. Peev, C. Pacher, R. Alléaume et al. // New Journal of Physics 11 (2009) 075001

ITMO UNIVERSITY

Что мы предлагаем?

Коммерчески доступные QKD-устройства	Bitrate (на 50 км), bit/s	Дальность	Возможность использования имеющихся телеком-каналов	Спектральная эффективность (достижимая)
1. Clavis3, idQuantique	3000	100 km	✓	~ 4%
2. Q-Box, MAGIQ	100	50 km	✗	~ 4%
3. Cygnus, SeQureNet	1000	80 km	✗	~ 4%
4. **Наша SCWQC система**	**40 000**	**250 km**	✓	**40-50%**

Ключевые преимущества нашего устройства:

- **Более высокая скорость передачи и большая дальность по сравнению с имеющимся на рынке аналогами**
- **Возможность использования имеющейся сетевой инфраструктуры:**
  - Простота: совместимость с существующими технологиями
  - Стоимость: нет необходимости в прокладке новых оптических линий
- **Высокая спектральная эффективность: до 50% в 10 Gbit Ethernet канале**

ITMO UNIVERSITY

Городские защищённые квантовые сети

- Диаметр Москвы 35-40 km

  На этом расстоянии прибор SCW QKD генерирует сигнал со скоростью **1 Mbit/s** (DWDM), аналоги: до 500 kbit/s

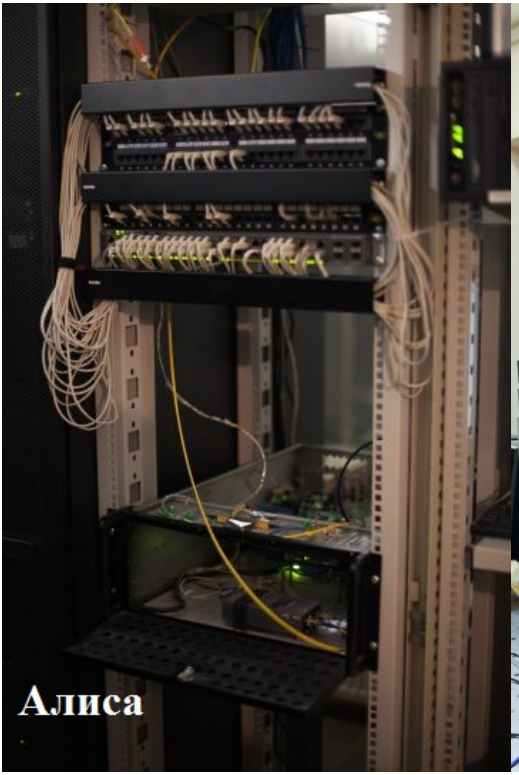
- Расстояние от Москвы до Петербурга составляет 620 km

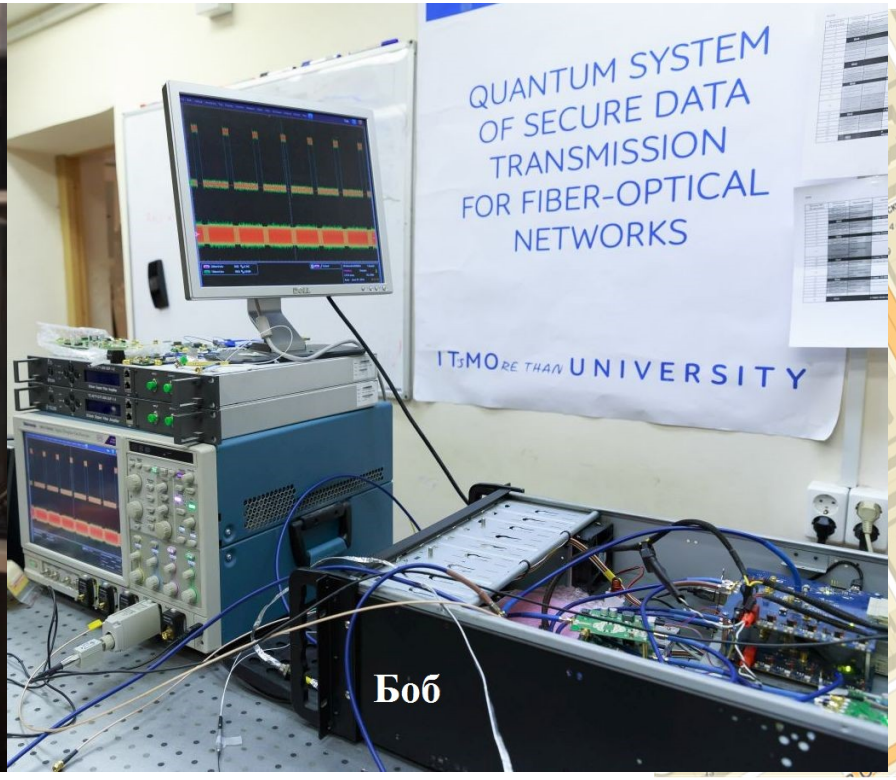
  Нужно **только 3** ретранслятора

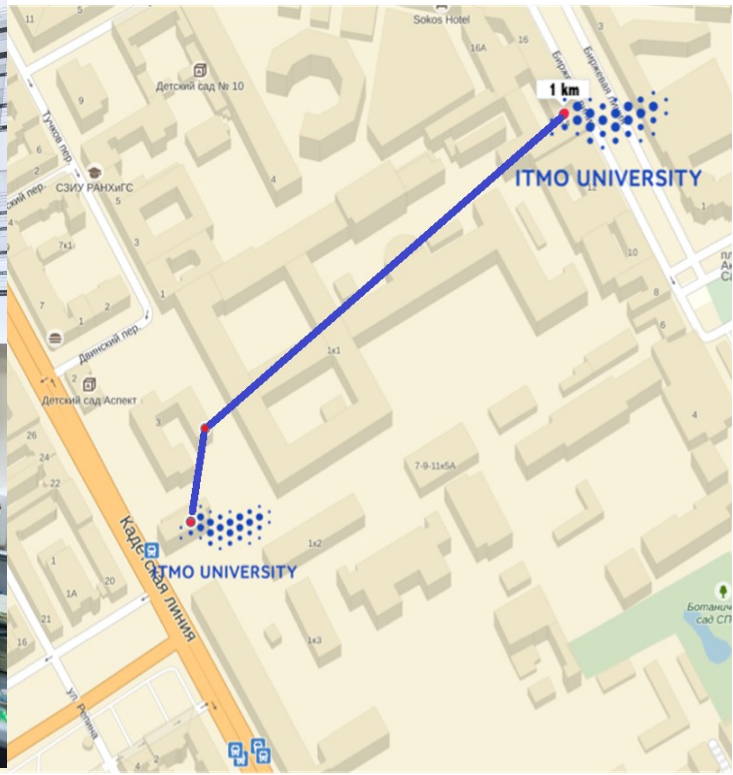
- **Не нужны специальные волокна**, встраивается в существующие линии связи!

ITMO UNIVERSITY

First Russian quantum network in metropolitan area







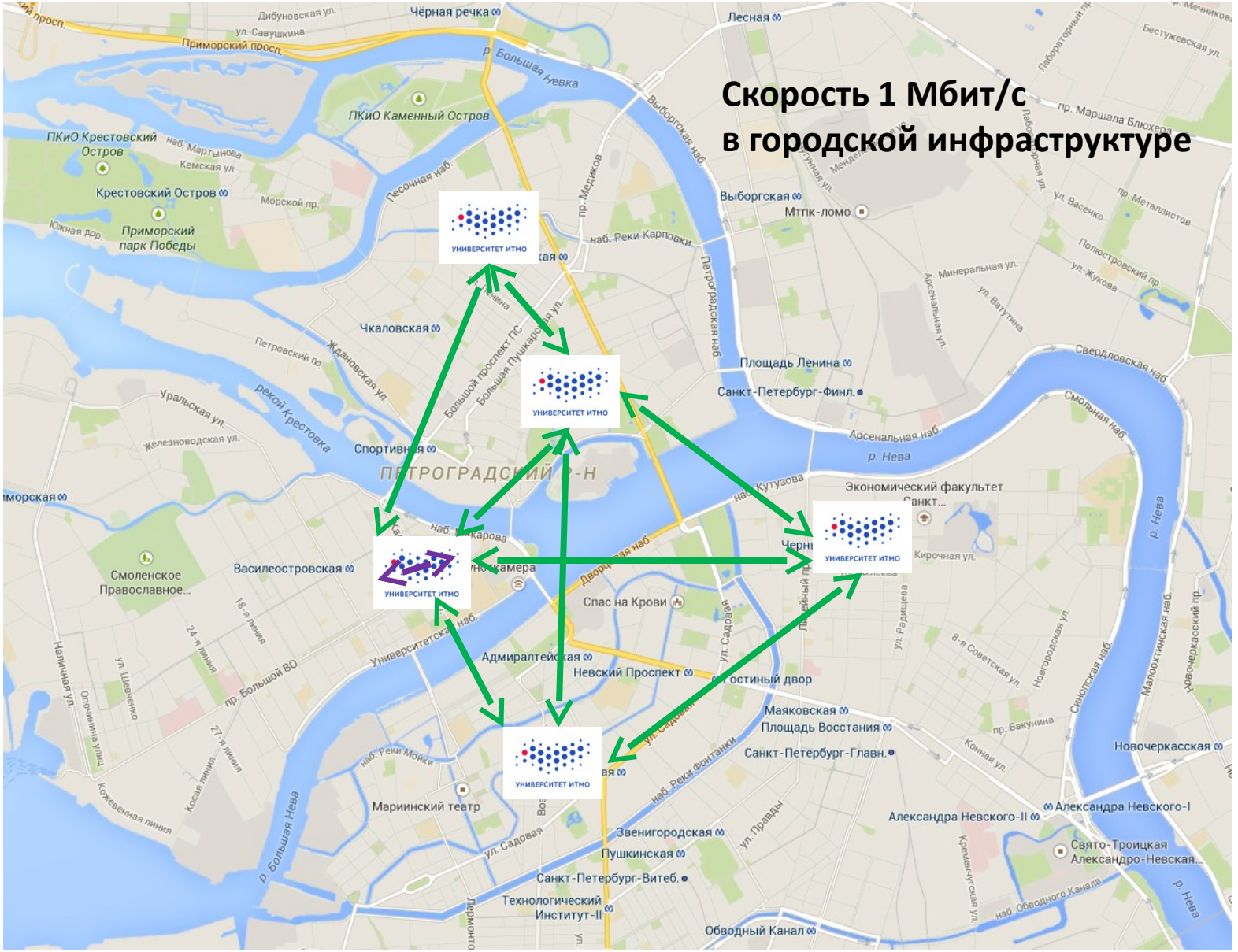
Parameters:
Number of nodes: 2
Channel loss: 1.6 dB;
Key rate: up to 1 Mbit/s;
QBER: 1%;
Medium: telecom optical cable (SMF-28 fiber)

2014 - Present

Location:
ITMO University
Saint Petersburg,
Vasilyevsky Island

ITMO UNIVERSITY

Квантовая криптография в городской инфраструктуре



ITMO UNIVERSITY

Испытательные полигоны

- **Санкт-Петербург** (Квантовая сеть Университета ИТМО) Опытный участок в действующей инфраструктуре

QUANTUM COMMUNICATIONS ITMO UNIVERSITY ВУЗТЕЛЕКОМЦЕНТР

- **Казань** (коллаборация с телеком оператором) Многоузловая квантовая сеть на основе метода на боковых частотах

KQC 2014 Kazan Quantum Center ТАТТЕЛЕКОМ ITMO UNIVERSITY

- **Самара** (коллаборация с ИТ-инфраструктурой) Создание программно-конфигурируемых квантовых сетей

ITMO UNIVERSITY open{code:} открытый код СМАРТС

ITMO UNIVERSITY

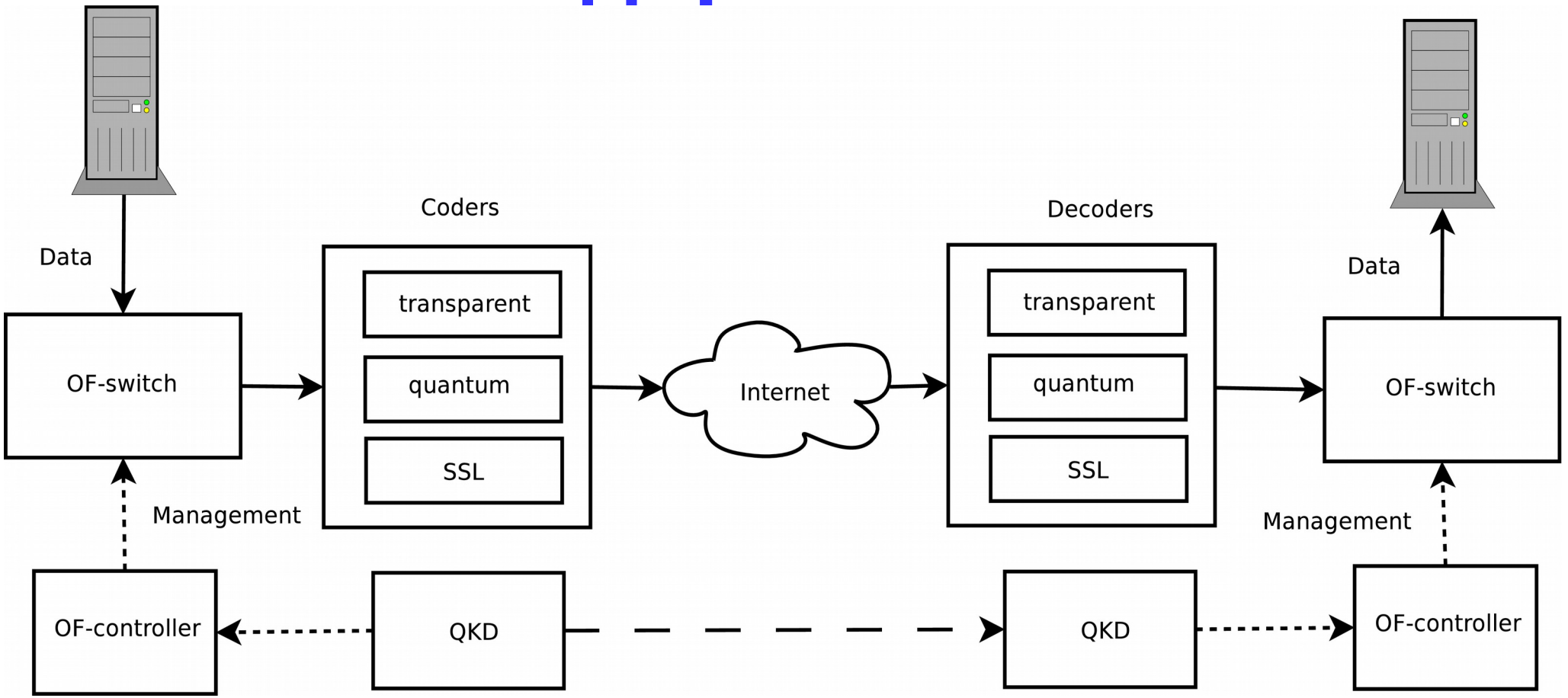
Quantum Networks + SDN

- Venkat R. Dasari, Travis S. Humble. OpenFlow Arbitrated Programmable Network Channels for Managing Quantum Metadata. https://arxiv.org/abs/1512.08545

- Venkat R. Dasari, Ronald J. Sadlier, Ryan Prout, Brian P. Williams, Travis S. Humble. Programmable Multi-Node Quantum Network Design and Simulation. Proc. SPIE 9873, Quantum Information and Computation IX, 98730B (2016). https://arxiv.org/abs/1604.01276

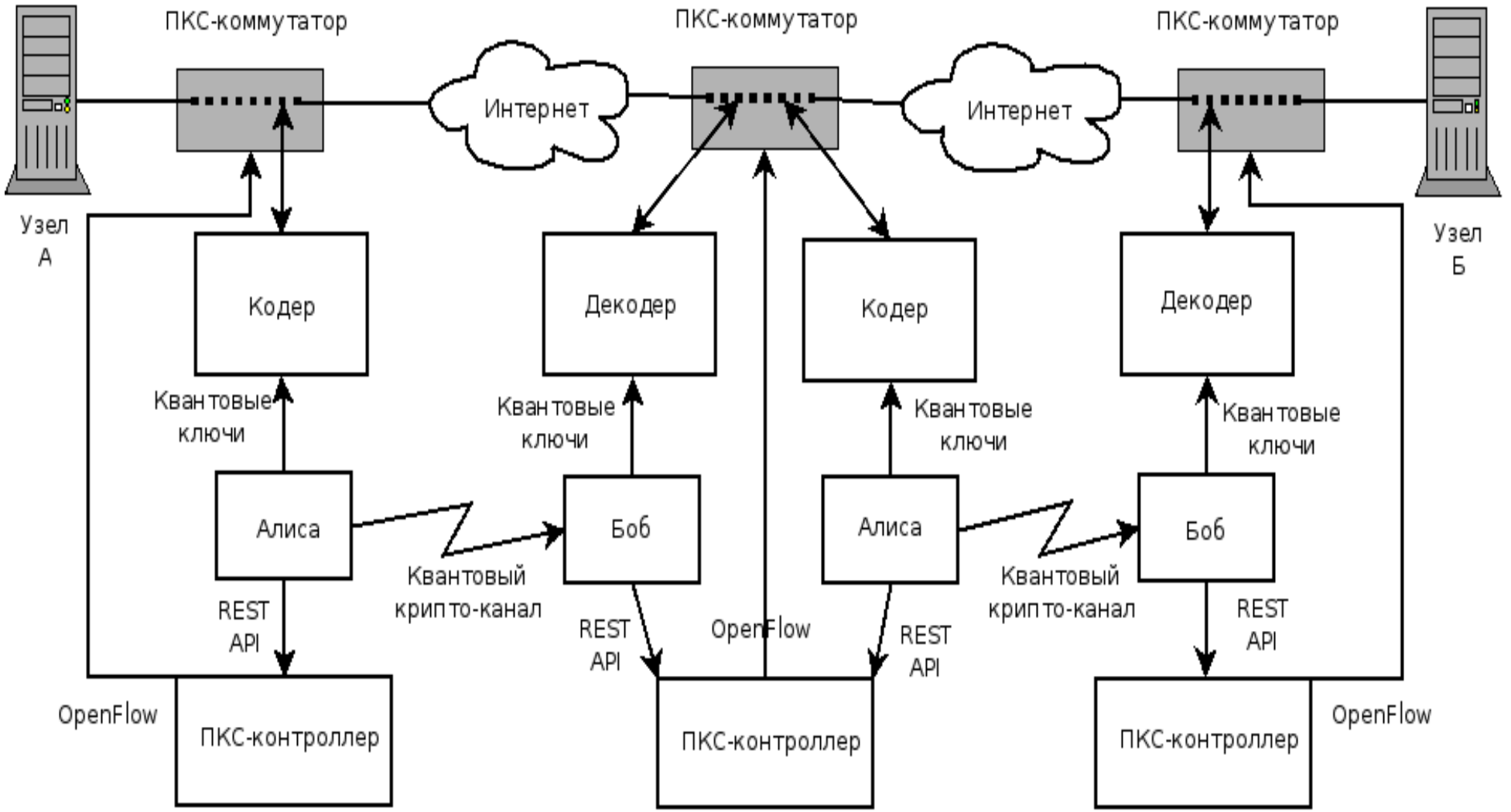
ITMO UNIVERSITY

Виртуальный канал кодирования



ITMO UNIVERSITY

Тестовая сеть



ITMO UNIVERSITY

Разработка

Узел:
- Linux драйвер
- QKD кодек
- Ryu application
- Тестовая сеть Mininet

3 узловая сеть:
- SW-switch
- HW-switch
- HW-switch + FPGA + кодек + OF-controller

Санкт-Петербург, Самара

ITMO UNIVERSITY

Работа выполняется при финансовой поддержке Минобрнауки РФ.
Соглашение о предоставлении субсидий от «27» октября 2015г. № 14.578.21.0112
Уникальный идентификатор ПНИЭР RFMEF157815X0112

sadov@mail.ifmo.ru
Олег Садов

http://sdn.ifmo.ru/