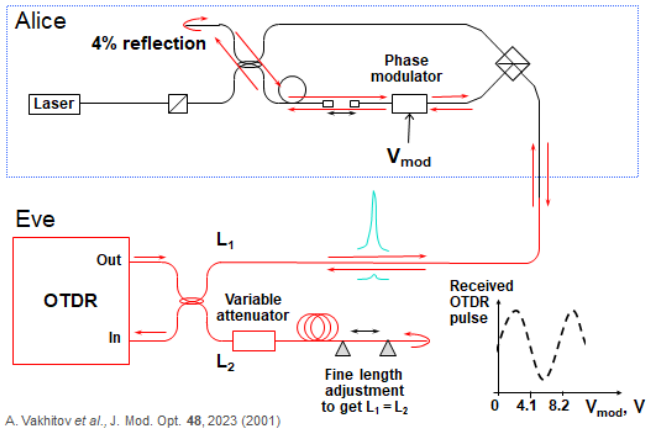
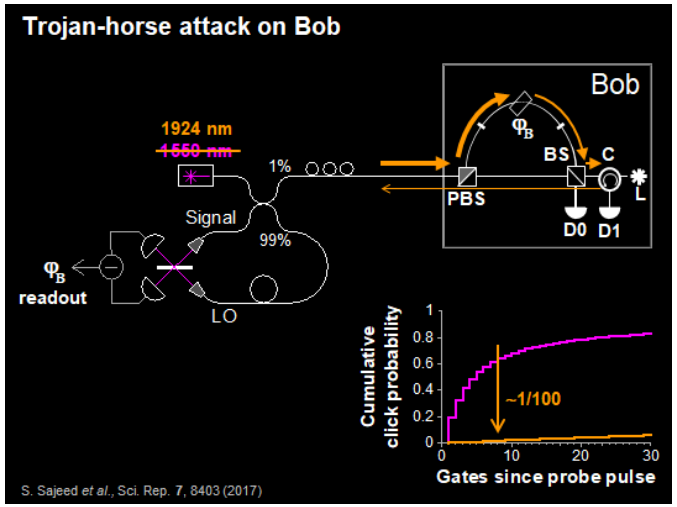
Взлом и сертификация квантовой криптографии

Trojan-horse attack experiment



A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001)



S. Sajeed *et al.*, Sci. Rep. **7**, 8403 (2017)

Вадим Макаров

Commercial QKD

1st generation (circa 2008)
ID Quantique *Cerberis* system

Classical encryptors:

L2, 2 Gbit/s
L2, 10 Gbit/s
L3 VPN, 100 Mbit/s

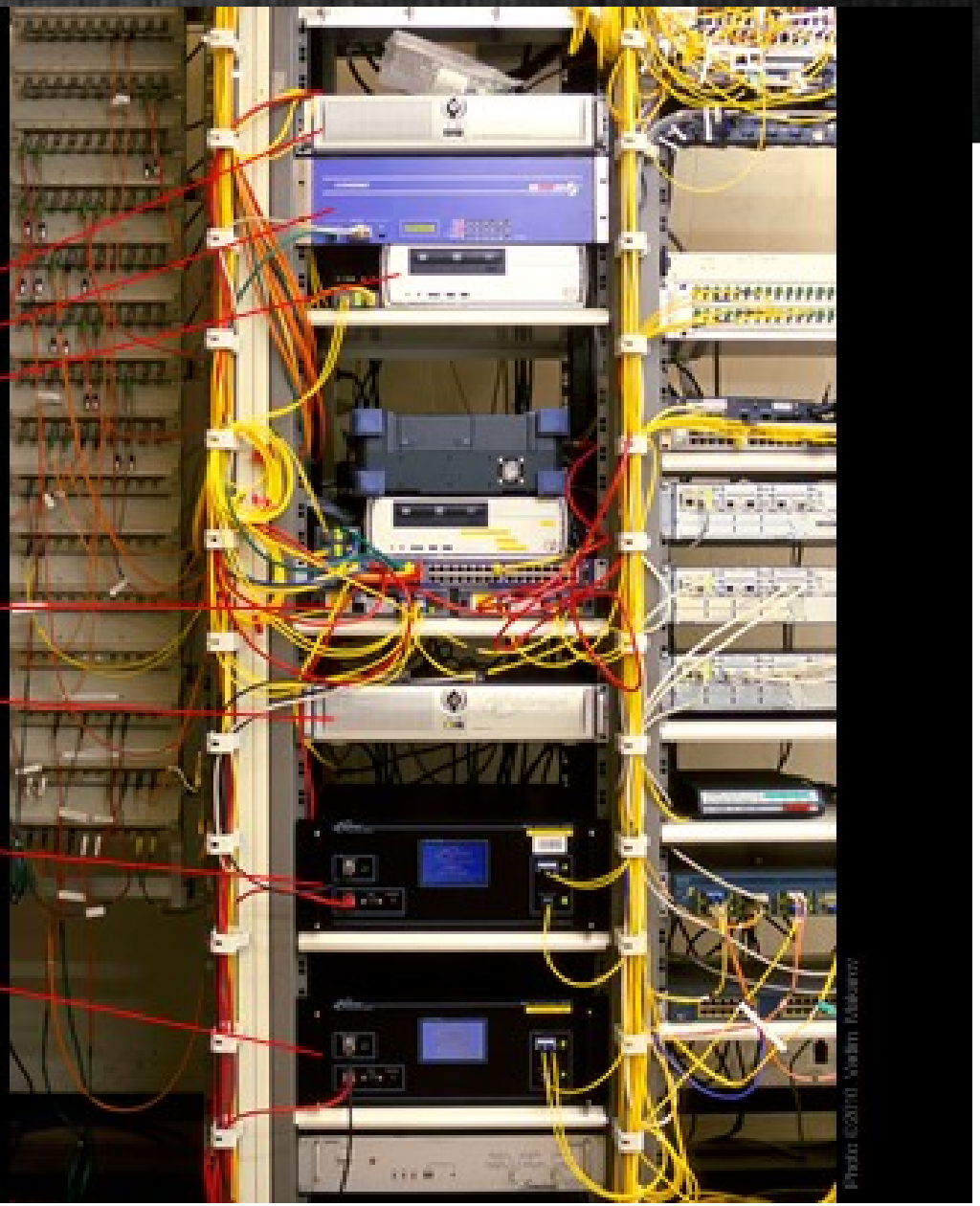
WDMs

Key manager

QKD to another node (4 km)

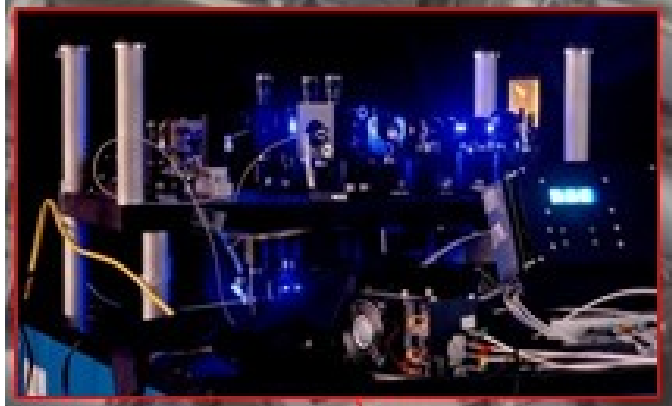
QKD to another node (14 km)

www.swissquantum.com



Eavesdropping 100% key on installed QKD line

on campus of the National University of Singapore, July 4–5, 2009



290 m of fiber

Eve

Alice

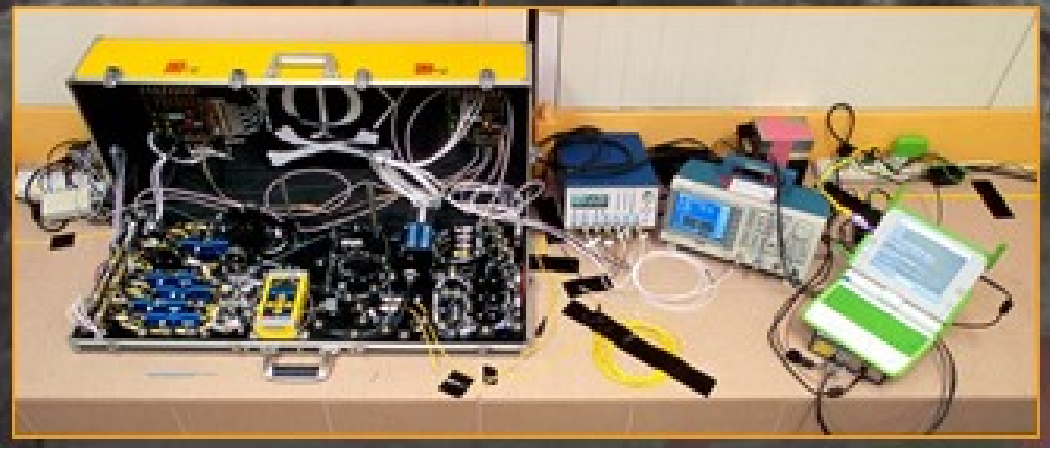
Bob

S15

S14

S13

S12



I. Gerhardt, Q. Liu *et al.*,
Nat. Commun. **2**, 349 (2011)

Российский квантовый центр

Квантовая связь в России

С 2014 года в России запущен проект в области наземной квантовой связи.
Инвнестиции до 450 000 000 рублей
31 мая 2016 года сотрудниками Российского квантового центра была запущена первая российская линия квантовой связи, созданная на базе оптоволоконной сети

Точки – отделения Газпромбанка на Коровьем валу и в Новых Черемушках.

Расстояние между зданиями около 30 км

Высокоскоростной квантовый шифратор МГУ

На базе технологии, созданной в рамках проекта Фонда перспективных исследований, будет создан высокопроизводительный шифратор с квантовым каналом распределения криптографических ключей для быстрой и абсолютно безопасной передачи информации по оптоволоконным линиям связи. *

* http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%92%D1%8B%D1%81%D0%BE%D0%BA%D0%BE%D1%81%D0%BA%D0%BE%D1%80%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D0%B9_%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D0%9C%D0%93%D0%A3

Испытания системы для квантовой защиты передачи данных на ВОЛС «Ростелекома»

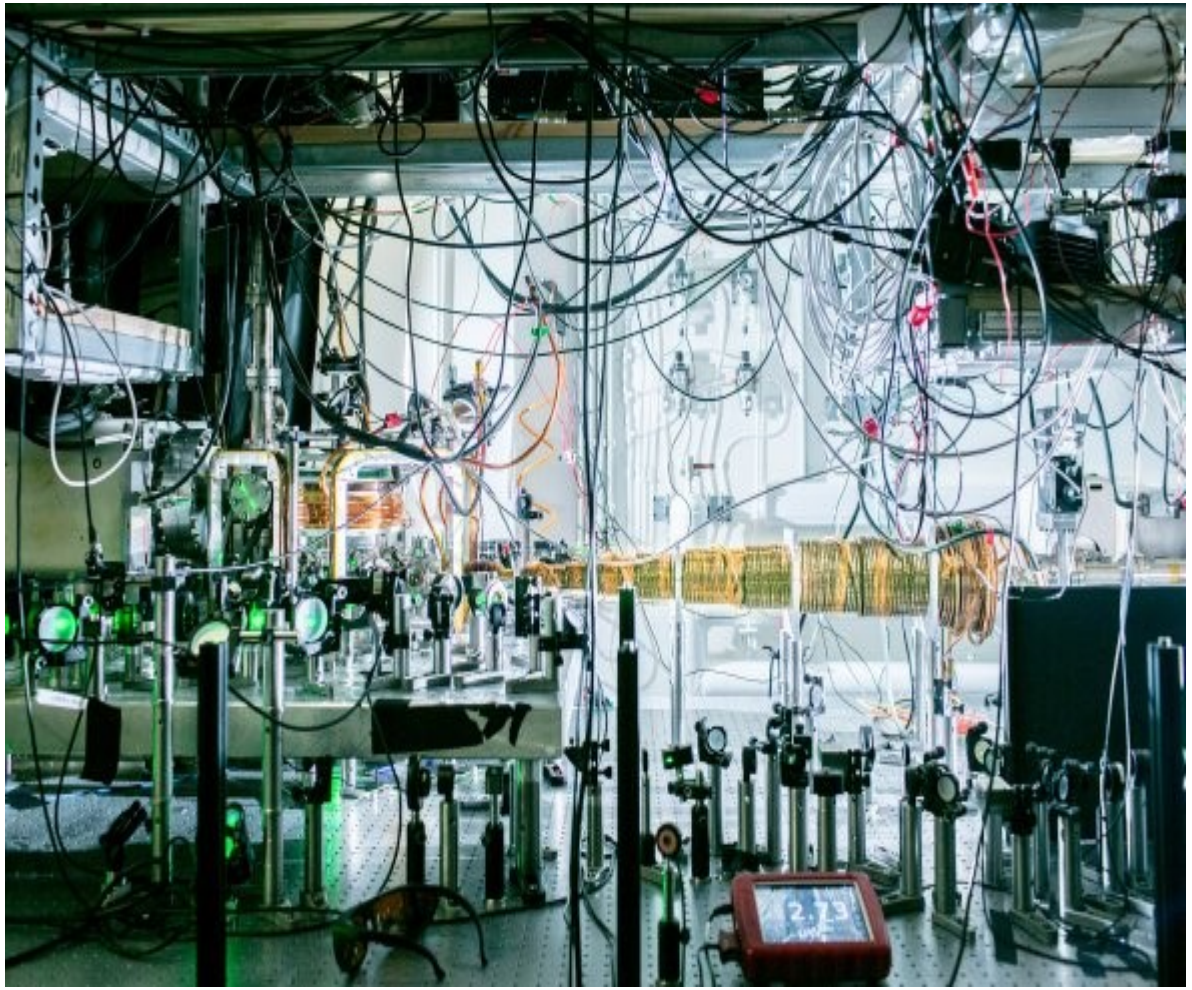
«Ростелеком» организовал в России опытную сеть передачи данных с квантовым шифрованием*

29 января 2019 года «Ростелеком» сообщил, что успешно провел второй этап испытаний отечественных оборудования и решений для организации квантовой защиты передачи данных на действующей волоконно-оптической линии связи (ВОЛС). Участниками тестирования стали Российский квантовый центр (РКЦ), компании QRate и «С-Терра СиЭсПи»**

*
http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_(%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)#.C2.AB.D0.A0.D0.BE.D1.81.D1.82.D0.B5.D0.BB.D0.B5.D0.BA.D0.BE.D0.BC.C2.BB_.D0.BE.D1.80.D0.B3.D0.B0.D0.BD.D0.B8.D0.B7.D0.BE.D0.B2.D0.B0.D0.BB_.D0.B2_.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D0.B8_.D0.BE.D0.BF.D1.8B.D1.82.D0.BD.D1.83.D1.8E_.D1.81.D0.B5.D1.82.D1.8C_.D0.BF.D0.B5.D1.80.D0.B5.D0.B4.D0.B0.D1.87.D0.B8_.D0.B4.D0.B0.D0.BD.D0.BD.D1.8B.D1.85_.D1.81_.D0.BA.D0.B2.D0.B0.D0.BD.D1.82.D0.BE.D0.B2.D1.8B.D0.BC_.D1.88.D0.B8.D1.84.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5.D0.BC

**http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:QRate_%D0%A0%D0%9A%D0%A6_%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9_%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%BE%D0%B9_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8#2019:_.D0.98.D1.81.D0.BF.D1.8B.D1.82.D0.B0.D0.BD.D0.B8.D1.8F_.D1.81.D0.B8.D1.81.D1.82.D0.B5.D0.BC.D1.8B_.D0.B4.D0.BB.D1.8F_.D0.BA.D0.B2.D0.B0.D0.BD.D1.82.D0.BE.D0.B2.D0.BE.D0.B9_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D1.8B_.D0.BF.D0.B5.D1.80.D0.B5.D0.B4.D0.B0.D1.87.D0.B8_.D0.B4.D0.B0.D0.BD.D0.BD.D1.8B.D1.85_.D0.BD.D0.B0_.D0.92.D0.9E.D0.9B.D0.A1_.C2.AB.D0.A0.D0.BE.D1.81.D1.82.D0.B5.D0.BB.D0.B5.D0.BA.D0.BE.D0.BC.D0.B0.C2.BB

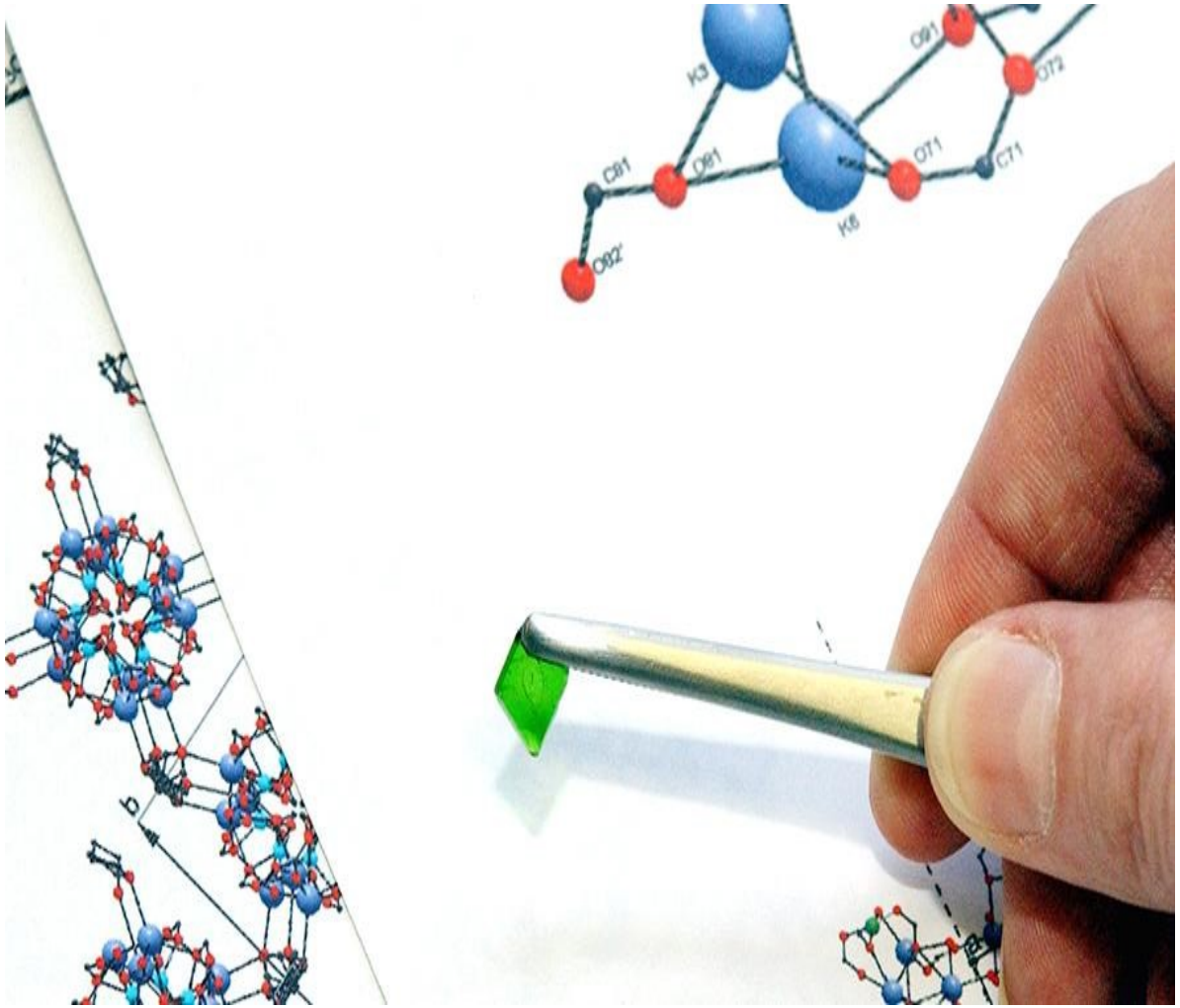
RQC изнутри: как устроен Российский квантовый центр



В 2011 году Российский квантовый центр (Russian Quantum Center, RQC) — такое название носит новая организация — получил грант от «Сколково» на 435 млн руб., и это первые и последние «государственные» деньги, которые привлекала компания. Всего за все время работы центр получил 1,5 млрд руб. инвестиций, в том числе 565 млн руб. от Газпромбанка.

https://www.rbc.ru/magazine/2018/01/5a3ccf2e9a79474240f50294

Квантовый компьютер в России появится через три года
Ранее предполагалось, что на это потребуется пять лет
7 мая 2018



В 2011 году Российский квантовый центр (Russian Quantum Center, RQC) — такое название носит новая организация — получил грант от «Сколково» на 435 млн руб., и это первые и последние «государственные» деньги, которые привлекала компания. Всего за все время работы центр получил 1,5 млрд руб. инвестиций, в том числе 565 млн руб. от Газпромбанка.

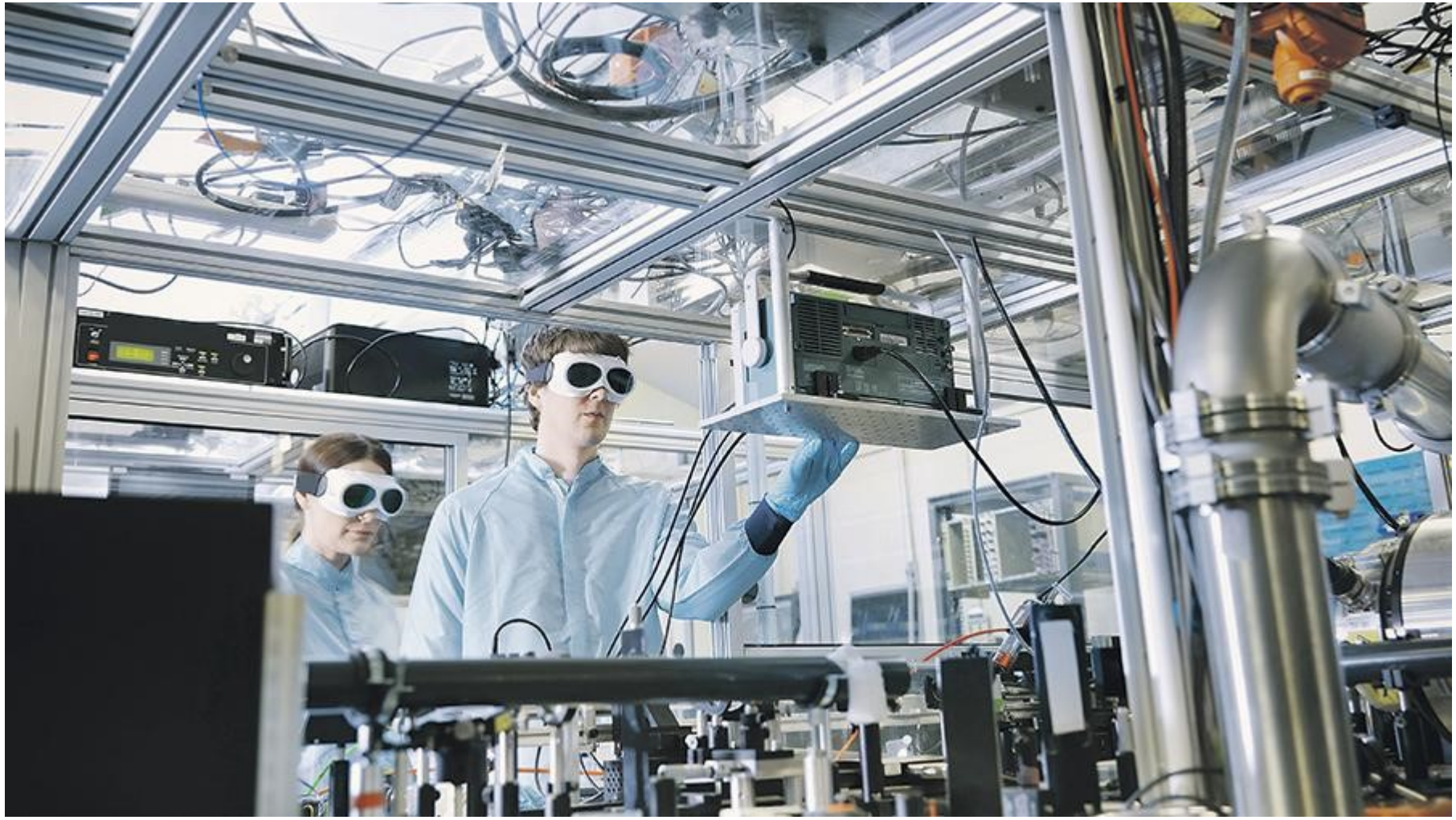
https://iz.ru/734210/mariia-nediuk/kvantovyi-kompiuter-v-rossii-poiavitsia-cherez-tri-goda

От исследований к реальному применению

- В России план развития квантовых технологий разработан до 2024 г.
- План предусматривает вложения в эту область более 43 млрд руб.
- Проект «дорожной карты» в мае представили Российский квантовый центр (РКЦ) и НИТУ МИСиС совместно с привлеченными экспертами.
- Примеры:
  - Volkswagen с Google и D-Wave используют квантовые компьютеры для решения задач оптимизации городского трафика.
  - Другая проблема— построение емких аккумуляторов (емскость>в 10 раз) для создания электромобилей. Одной из основных сфер применения квантовых компьютеров на первых этапах называют моделирование новых материалов.

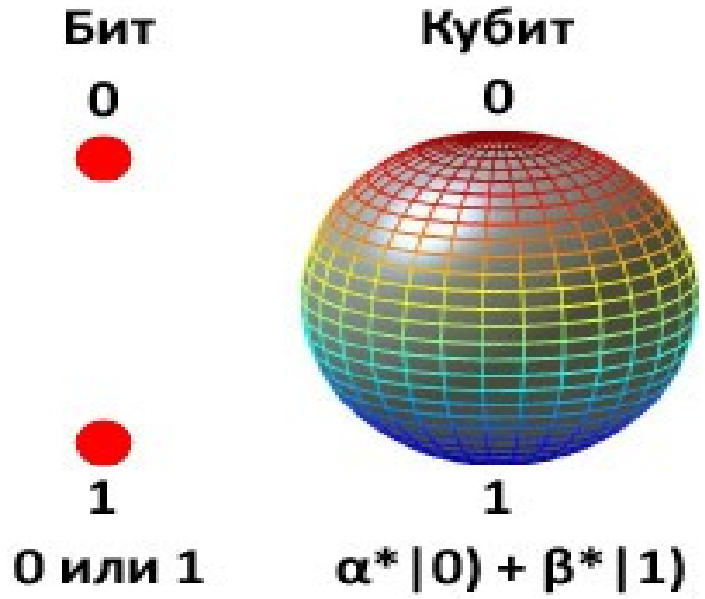
https://www.kommersant.ru/doc/3976880

2018 год. Квантовый компьютер и усилитель



Устранены помехи на пути к квантовому компьютеру
Созданный отечественными физиками усилитель значительно ускорит работу вычислительной машины будущего

Квантово-устойчивая криптография



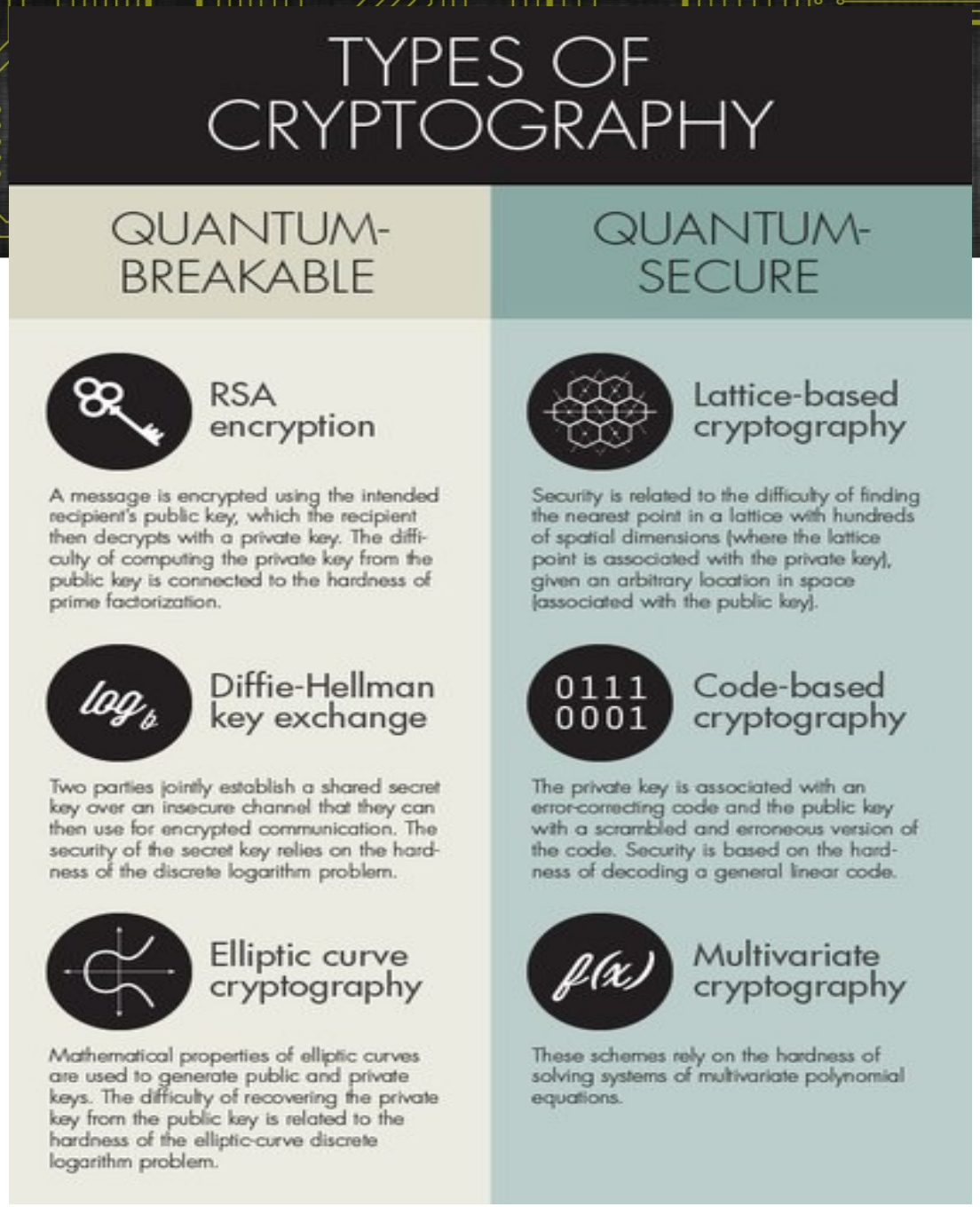
Сейчас существует 6 различных подходов:

- Lattice-based cryptography
- Multivariate cryptography
- Hash-based cryptography
- Code-based cryptography
- Supersingular Elliptic Curve Isogeny cryptography
- Symmetric Key Quantum Resistance

Ежегодная конференция PQCrypto (https://twitter.com/pqcryptoconf, 10th edition in 2019)

(по материалам PHDays 2019)

Квантово-устойчивая криптография



https://en.wikipedia.org/wiki/Lattice-based_cryptography*

Пример:

- Lattice-based cryptography – решетчатая криптография*
- Считается безопасной в предположении, что некоторые хорошо изученные задачи вычислительной решетки не могут быть эффективно решены.

(по материалам PHDays 2019)*

https://www.wired.com/2015/09/tricky-encryption-stump-quantum-computers/ **

Постквантовая криптография (wiki)

- часть криптографии, которая остаётся актуальной и при появлении квантовых компьютеров и квантовых атак, поскольку по скорости вычисления традиционных криптографических алгоритмов квантовые компьютеры значительно превосходят классические компьютерные архитектуры
- современные криптографические системы становятся потенциально уязвимыми для криптографических атак. Большинство традиционных криптосистем опирается на проблемы факторизации целых чисел или задачи дискретного логарифмирования, которые будут легко разрешимы на достаточно больших квантовых компьютерах, использующих алгоритм Шора.[1][2] Многие криптографы в настоящее время ведут разработку алгоритмов, независимых от квантовых вычислений, то есть устойчивых к квантовым атакам.

Постквантовая криптография

- Существуют классические криптосистемы, опирающиеся на вычислительно сложные задачи и имеют ряд существенных отличий от классических систем сильной криптографии. Из-за этого их гораздо сложнее решить. Эти системы независимы от квантовых вычислений, и, следовательно, их считают квантово-устойчивыми (quantum-resistant), или «постквантовыми» криптосистемами.
- Постквантовая криптография в свою очередь отличается от квантовой криптографии, которая занимается методами защиты коммуникаций, основанных на принципах квантовой физики.

https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D1%82%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F

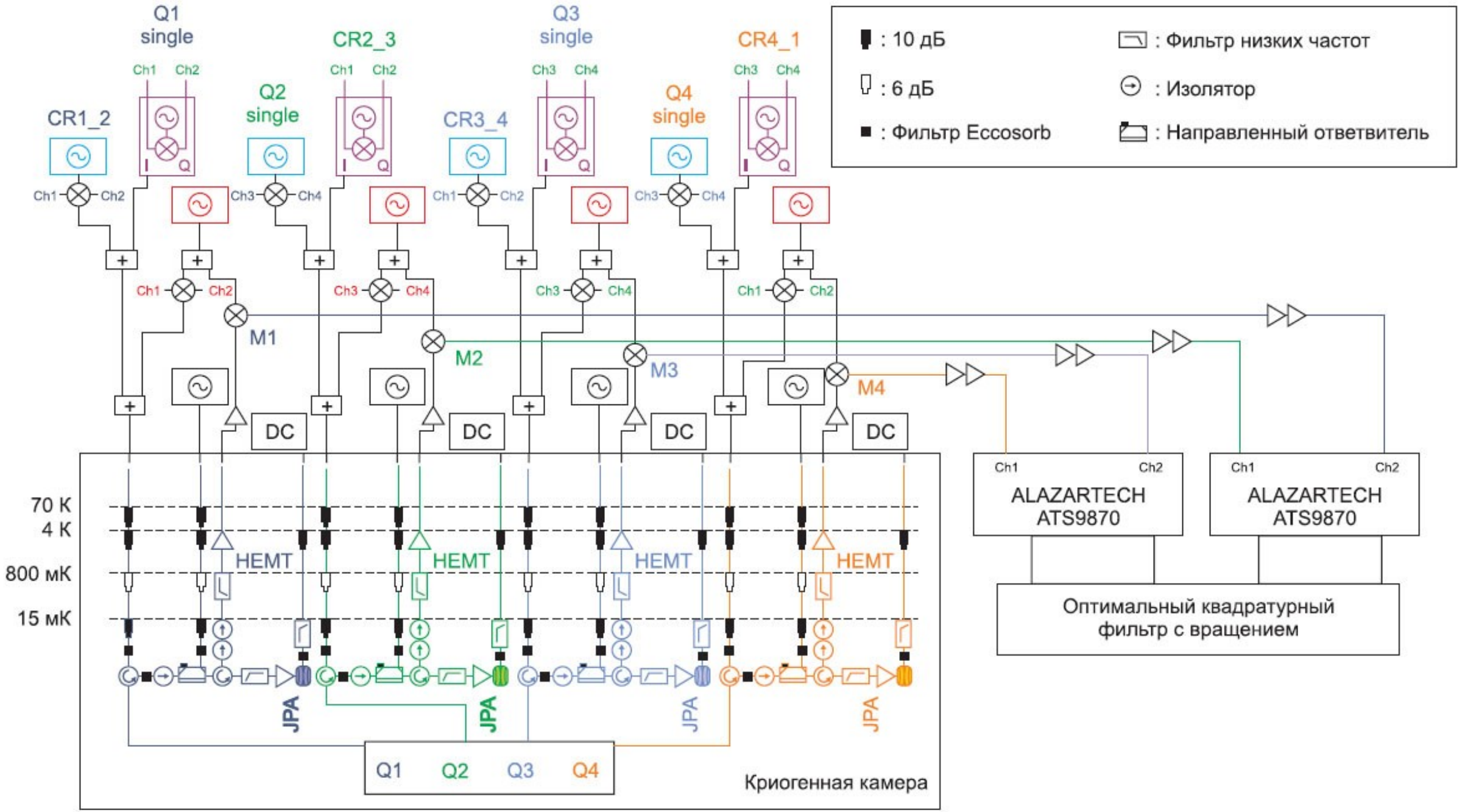
Квантово-устойчивые асимметричные алгоритмы

Квантово-устойчивых асимметричных алгоритмов очень мало. Наиболее известный из них NTRU, основанный на lattice-based shortest vector problem:

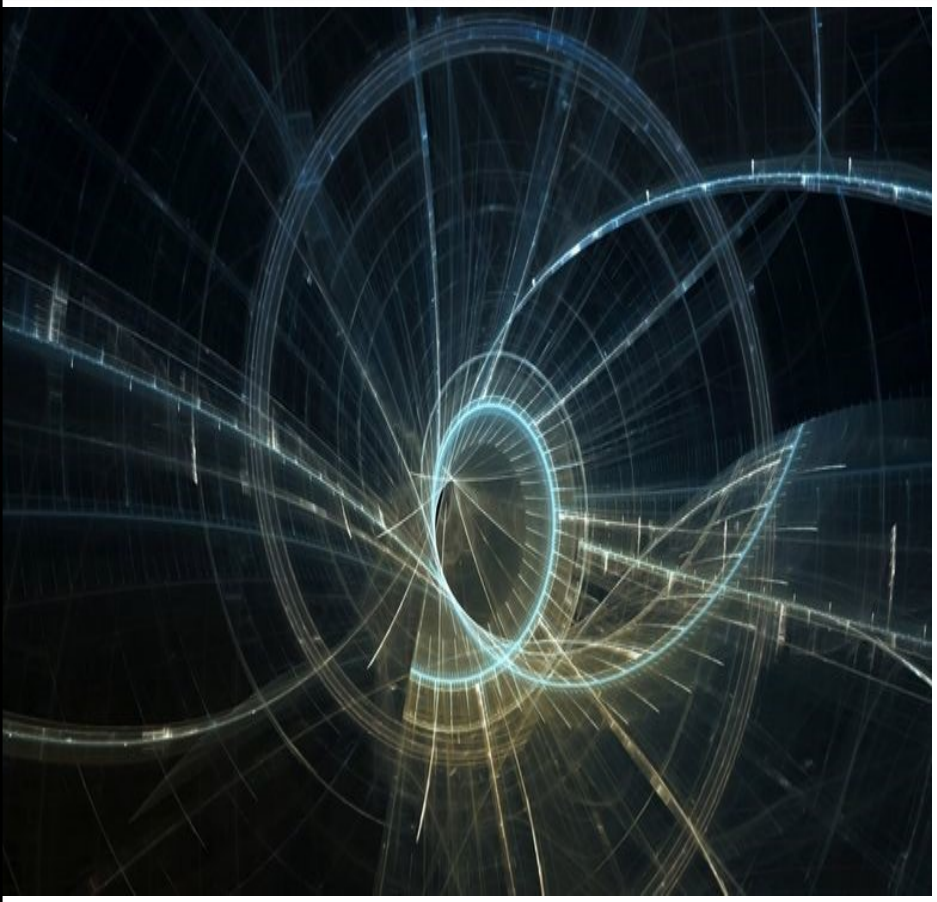
- NTRUEncrypt для шифрования
- NTRUSign для цифровой подписи

*https://www.onboardsecurity.com/products/ntru-crypto

(по материалам PHDays 2019)


Q1 single
CR2_3
Q3 single
CR4_1
CR1_2
Q2 single
CR3_4
Q4 single
Ch1 Ch2
Ch3 Ch4
M1
M2
M3
M4
DC
70 K
4 K
800 мК
15 мК
HEMT
JPA
Q1 Q2 Q3 Q4
Криогенная камера
ALAZARTECH ATS9870
ALAZARTECH ATS9870
Оптимальный квадратурный фильтр с вращением
: 10 дБ
: 6 дБ
: Фильтр Eccosorb
: Фильтр низких частот
: Изолятор
: Направленный ответвитель

Приложения



- “зоопарк языков программирования” - https://www.americanscientist.org/article/programming-your-quantum-computer
- языки квантового программирования в википедии https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5
- Квантовая сеть https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C

Квантовая информатика

- Раздел науки, возникший в конце XX века на стыке квантовой механики, теории алгоритмов и теории информации.
- В квантовой информатике изучаются общие принципы и законы, управляющие динамикой сложных квантовых систем[1]. Моделью таких систем является квантовый компьютер.
- Квантовая информатика включает в себя вопросы квантовых вычислений и квантовых алгоритмов, физику квантовых компьютеров, квантовой криптографии и квантовой теории информации, непосредственно касается оснований квантовой теории, в частности, проблемы измерений и описания декогерентности.
- Важнейшим физическим явлением, которое изучается в квантовой информатике, является запутанные квантовые состояния и порождаемые ими нелокальные свойства квантовой физики многих тел.

Новая разработка вывела российский квантовый компьютер на мировой уровень

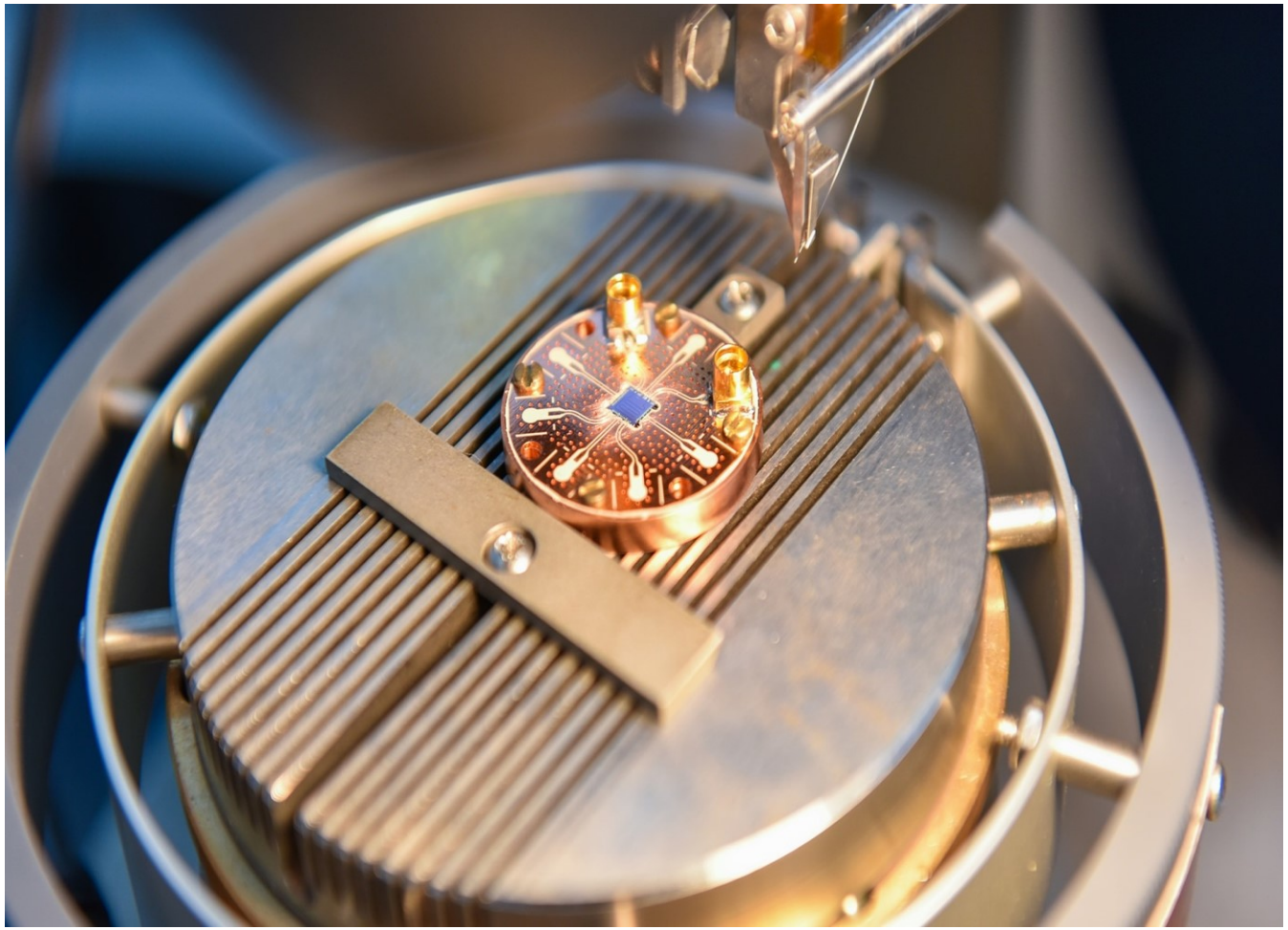


Фото пресс-службы НИТУ "МИСиС".

Создание усилителя с минимальным уровнем шума стало одной из ключевых задач в ходе построения квантового компьютера.

Физики лаборатории "Сверхпроводящие метаматериалы" НИТУ "МИСиС" и двух институтов РАН создали самый качественный в мире усилитель сигнала для квантового компьютера. Устройство может применяться также в радиотелескопах и других приборах, работающих со сверхслабым радиоизлучением.

Физики сделали из сверхпроводника "кота Шрёдингера" для квантовых компьютеров

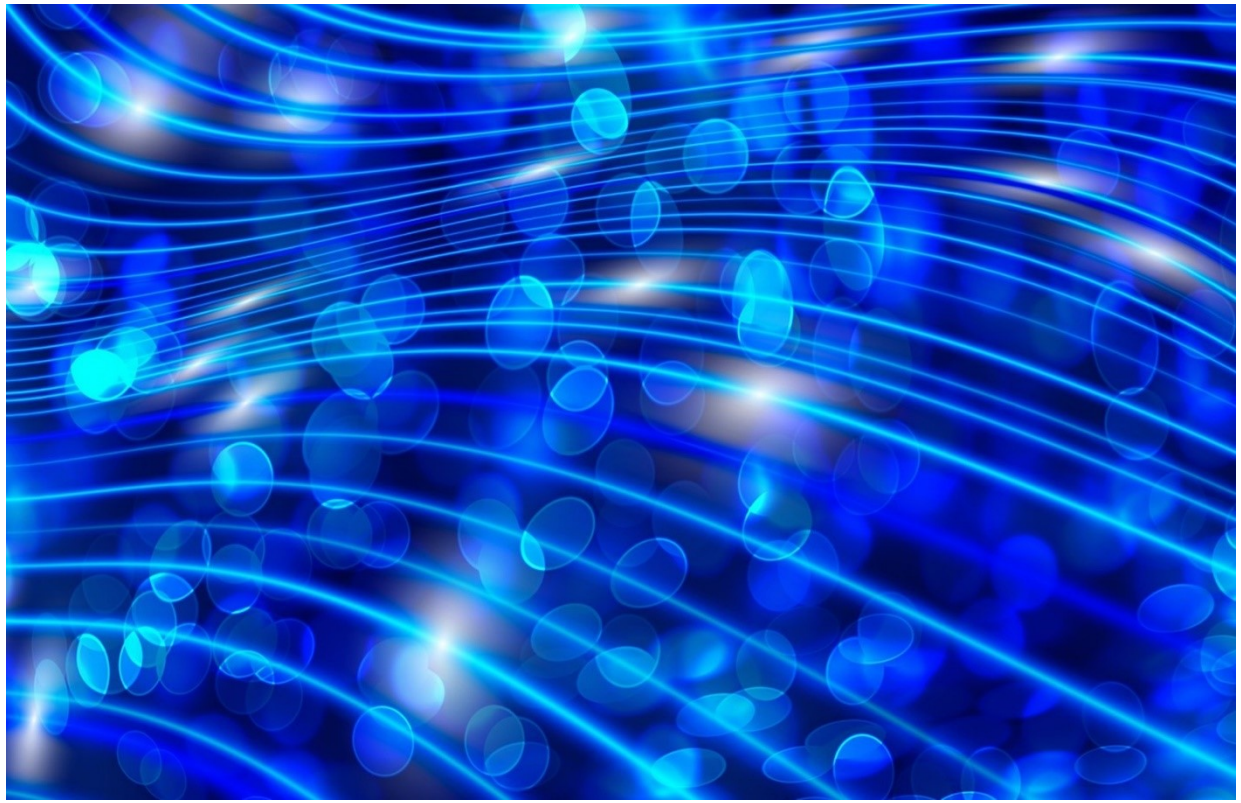


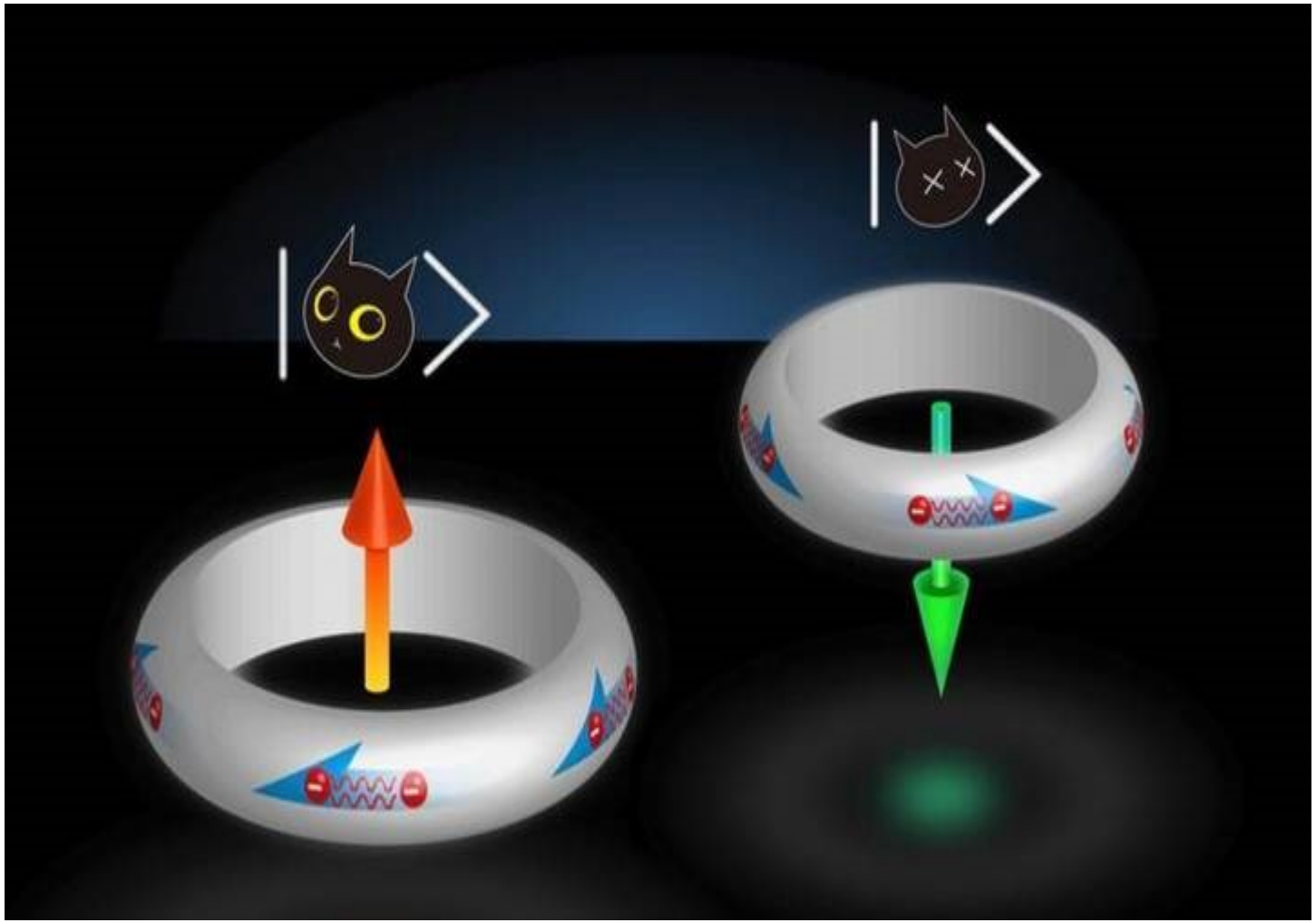
Иллюстрация Johns Hopkins University

Материалы с особыми свойствами могут служить для физической реализации кубита.

Физики разработали новый перспективный тип кубитов из сверхпроводящего материала. Это достижение приближает эру квантовых вычислений.

Подробности описаны в научной статье, опубликованной в журнале Science группой во главе с Чиа-Лин Чянем (Chia-Ling Chien) из Университета Джона Хопкинса.

Кубит, как знаменитый кот Шрёдингера, может находиться в комбинации двух, казалось бы, взаимоисключающих состояний

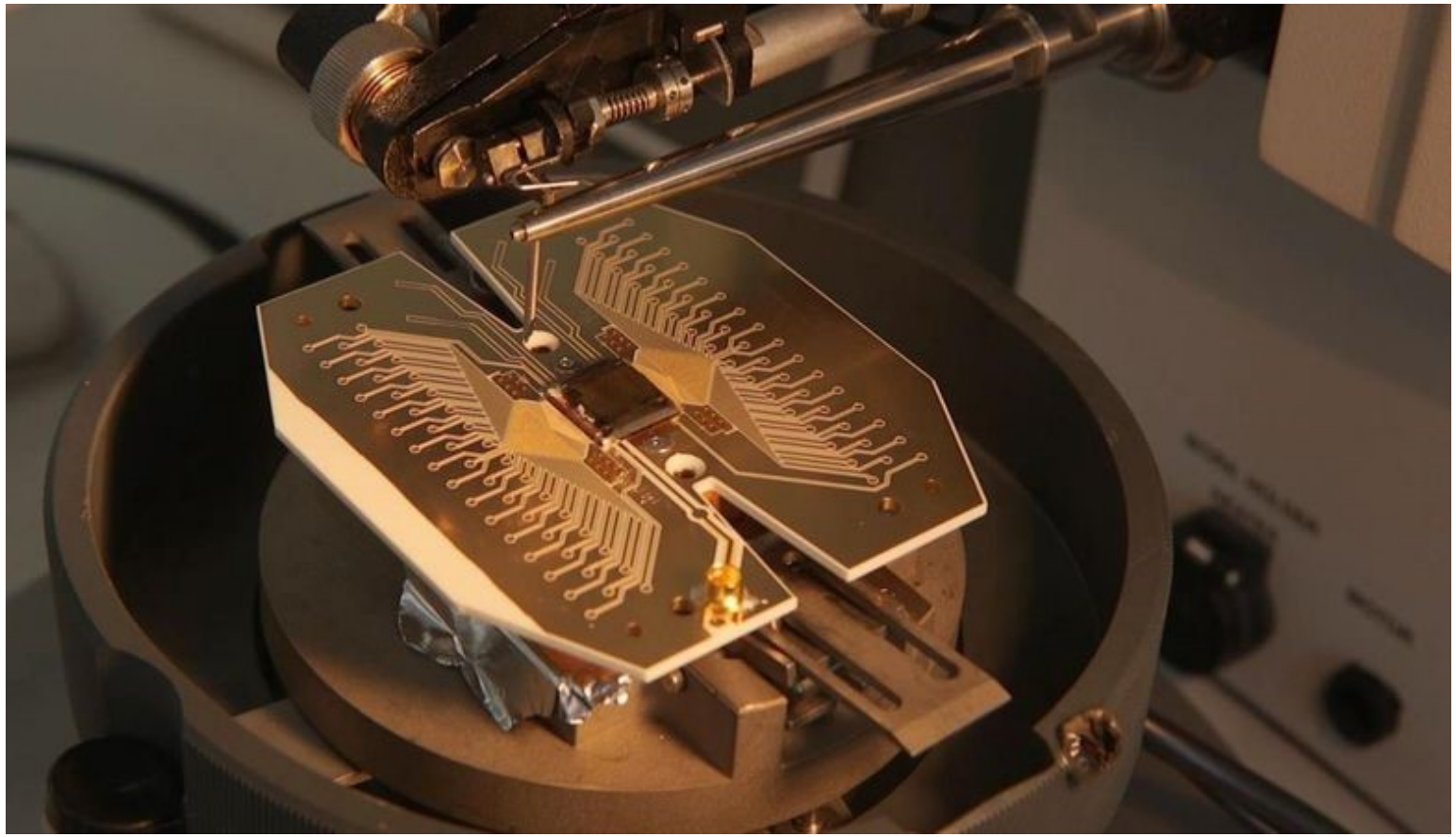


Материалы с особыми свойствами могут служить для физической реализации кубита.

Физики разработали новый перспективный тип кубитов из сверхпроводящего материала. Это достижение приближает эру квантовых вычислений.

Подробности описаны в научной статье, опубликованной в журнале Science группой во главе с Чиа-Лин Чянем (Chia-Ling Chien) из Университета Джона Хопкинса.

Языки программирования для квантового компьютера



Прототип ядра ионного квантового компьютера. Ion Quantum Technology Group, Сассекский университет

Несколько лет назад IBM дала возможность любому подключиться к 5-кубитному компьютеру. В проекте зарегистрировались 70 000 человек.

http://www.research.ibm.com/quantum/

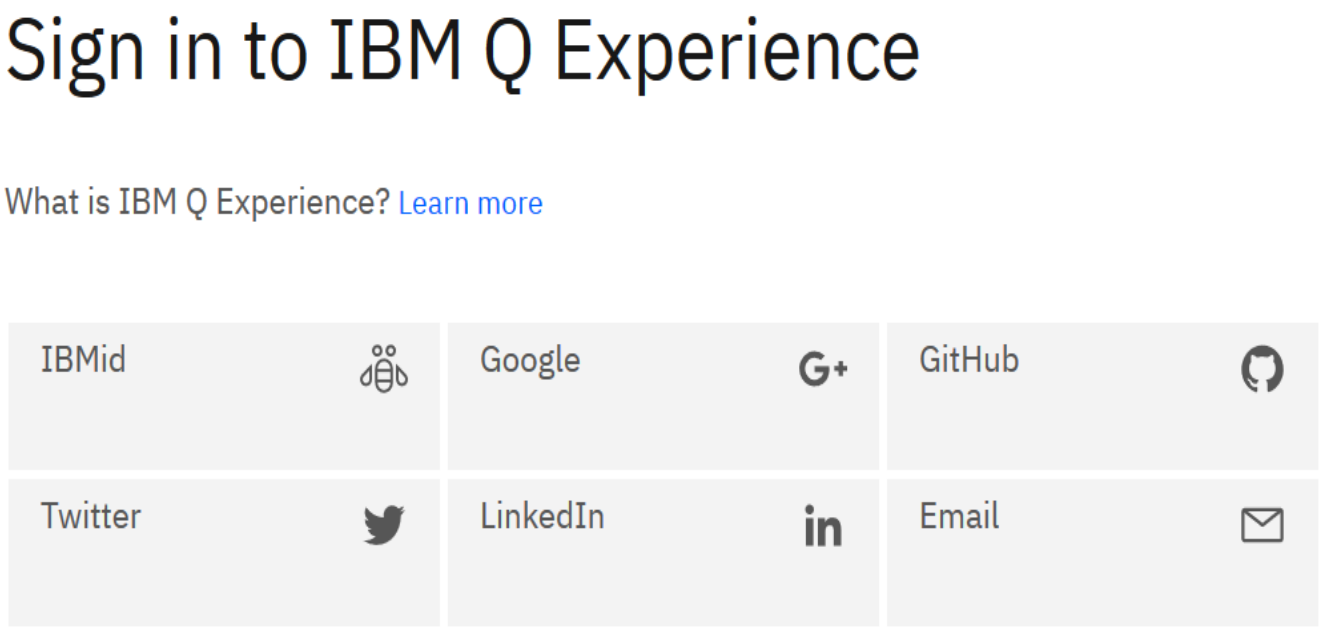
Тур в IBM Q Lab

IBM представляет облачную платформу квантовых вычислений под названием IBM Quantum Experience, чтобы позволить исследователям и научному сообществу экспериментировать на квантовом процессоре, чтобы помочь обнаружить новые приложения для этой технологии.

http://ibm.com/quantumcomputing

https://www.youtube.com/watch?v=KZf4BSmgdO4&feature=youtu.be

IBM анонсирует облачную платформу квантовых вычислений



(Tech Xplore) —IBM объявила о разработке платформы квантовых вычислений, которая позволит пользователям получать доступ и программировать свой 5-кубитовый квантовый компьютер через Интернет.

Компания, получившая название IBM Quantum Experience, утверждает, что это первая в мире система, которая позволяет внешним пользователям работать с квантовым компьютером через облако.

https://quantum-computing.ibm.com/

AMERICAN Scientist

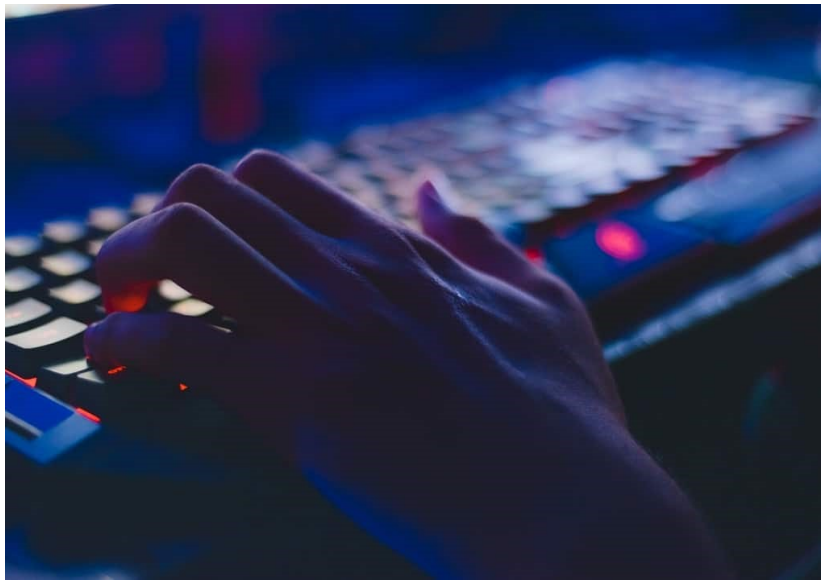
Programming Your Quantum Computer

BY BRIAN HAYES

The hardware doesn't yet exist, but languages for quantum coding are ready to go.

COMPUTER • TECHNOLOGY • INFORMATION THEORY

Где учиться программированию на квантовом компьютере*



1. Introduction to Quantum Computing by St Petersburg State University (Coursera)
2. QC101 Quantum Computing & Quantum Physics for Beginners (Udemy)
3. Quantum Computing: Theory to Simulation and Programming (Udemy)
4. Quantum Computing Courses (Udemy)
5. The Quantum World by Harvard University (edX)
6. The Building Blocks of a Quantum Computer by TU Delft (edX)
7. Quantum Computing Introduction by TU Delft (edX)
8. Turn Quantum Computing Knowledge into Action (MIT xPRO)

* https://digitaldefynd.com/best-quantum-computing-courses/

Microsoft Quantum Development Kit Samples*

Getting started

If you're new to quantum or to the Quantum Development Kit, we recommend starting with the Getting Started samples.

Going further

As you go further with quantum development, we provide several different categories of samples for you to explore:

- **Algorithms**: These samples demonstrate various quantum algorithms, such as database search and integer factorization.
- **Arithmetic**: These samples show how to coherently transform arithmetic data.
- **Characterization**: These samples demonstrate how to learn properties of quantum systems from classical data.
- **Chemistry**:
- **Diagnostics**: These samples show how to diagnose and test Q# applications.
- **Error Correction**: These samples show how to work with quantum error correcting codes in Q# programs.
- **Interoperability**: These samples show how to use Q# with different host languages.
- **Numerics**: The samples in this folder show how to use the numerics library.
- **Runtime**: These samples show how to work with the Q# simulation runtime.
- **Simulation**: These samples show how to simulate evolution under different Hamiltonians.

We also encourage taking a look at the unit tests used to check the correctness of the Quantum Development Kit samples.

Docker image

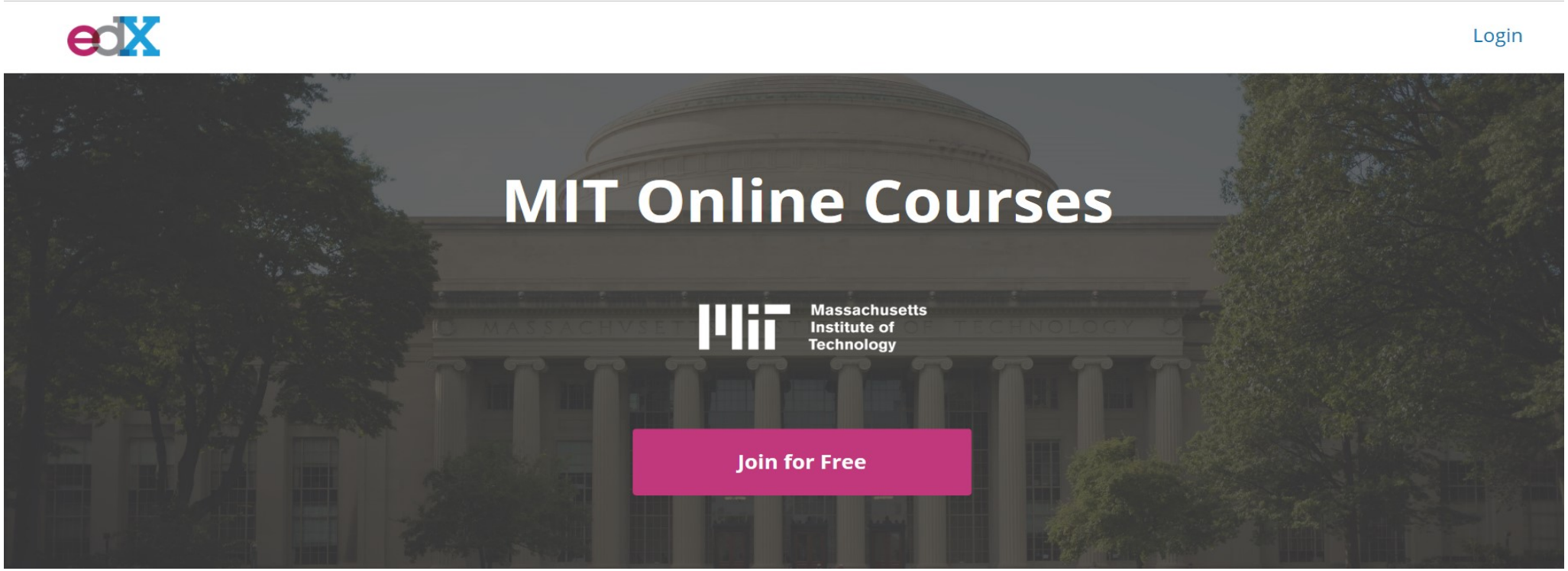
Лаборатория искусственных квантовых систем

Лаборатория искусственных квантовых систем (ИКС) создана в апреле 2014 года по результатам открытого конкурса МФТИ, проведенного в целях реализации программы повышения конкурентоспособности "5-100".

ЛАБОРАТОРИЯ ИСКУССТВЕННЫХ КВАНТОВЫХ СИСТЕМ

Основные задачи лаборатории ИКС - проведение научных исследований в области экспериментальной физики наноструктур и развитие сверхпроводниковых квантовых технологий, а также обучение студентов и аспирантов современным методам экспериментальной физики. С помощью квантовых технологий можно обеспечить революционные прорывы в области вычислений в интересах современного материаловедения, криптографии, оптимизации различных процессов. Все это определяет несомненную важность и перспективность задач, решаемых лабораторией ИКС.

Где учиться программированию на квантовом компьютере в Рф. Важно – учиться бесплатно, не платить за повышение квалификации: деньги с вас возьмут, а квалификация – ваше дело



- MIT на бесплатных онлайн курсах
- Coursera, можно в class central https://www.classcentral.com/subject/quantum-mechanics
- ресурсы github, gitlab
- Обязательно - электронные книги, вспомнить квантовую механику, следить за новостями, программировать