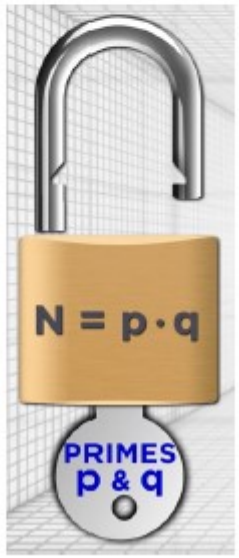
Когда Quantum сломает криптографию с открытым ключом?

Quantum Break



Простое число - это любое целое число большее 1, которое нацело делится только на единицу или на себя: 2,3,5,7,11,13,17,23,29,31, и т.д.
Традиционная сильная криптография с открытым ключом (например, RSA, Diffie-Hellman и т. д.) основана на трудостях решения уравнений с простыми числами (факторизация):
p * q = n, p и q - простые числа, n - открытый ключ, может быть очень трудно разложить на простые множители большое число.
Простой пример: 3 x 5 = 15
Другой простой пример:

- p*q=187, чему равны p и q?
- Ответ: p и q равны 17 и 11
- p*q= 84773093, чему равны p и q?
- Ответ: p и q равны 9539 и 8887

Еще один простой пример: Предположим, что n = p*q, длина n равна 2048 бит. Традиционные компьютеры будут очень долго вычислять p и q.

Как квантовые компьютеры делают это?

Простой перебор значений - 2^N вычислений, по одному за раз.

Если N = 2048, то 2^N = 3.2 * 10^{616}.

Формулы оценки скорости обычно выглядят как O(…). Это дает только оценку порядка, но если посчитать число внутри скобок, то получим:

- Для оптимизированного алгоритма на традиционном компьютере - 6.8 * 10^{51}
- Для квантового алгоритма Шора - 1.6 * 10^8, что гораздо меньше.

При этом потребуется квантовый регистр длиной 4097 кубит.

Когда Quantum сломает криптографию с открытым ключом?

Многие квантовые физики думают о появлении стабильных кубитов в течение 5 лет (если это еще не сделано) для взлома классической криптографии, использующей проблему факторизации для защиты данных.

Эффективность взлома

Алгоритм	Длина ключа	Уровень безопасности	
		обычный компьютер	Квантовый компьютер
RSA-1024	1024	80	~0
RSA-2048	2048	112	~0
ECC-256	256	128	~0
ECC-384	384	192	~0
AES-128	128	128	~64
AES-256	256	256	~128

Таблица приведена согласно материалам ISSA-конференции за апрель 2017 года, где был обозначен пятилетний временной горизонт для классических криптографических алгоритмов. С тех пор уже прошло два года.

Как противостоять взлому

Два направления “квантовой устойчивости”

Квантовое распределение ключей

- Алгоритм BB84
- Алгоритм E91
- Достижения в квантовом распределении ключей (Китай, Россия, США, Канада, европейские страны…)
- Российский квантовый центр, ИТМО и др.

Новые устойчивые алгоритмы

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

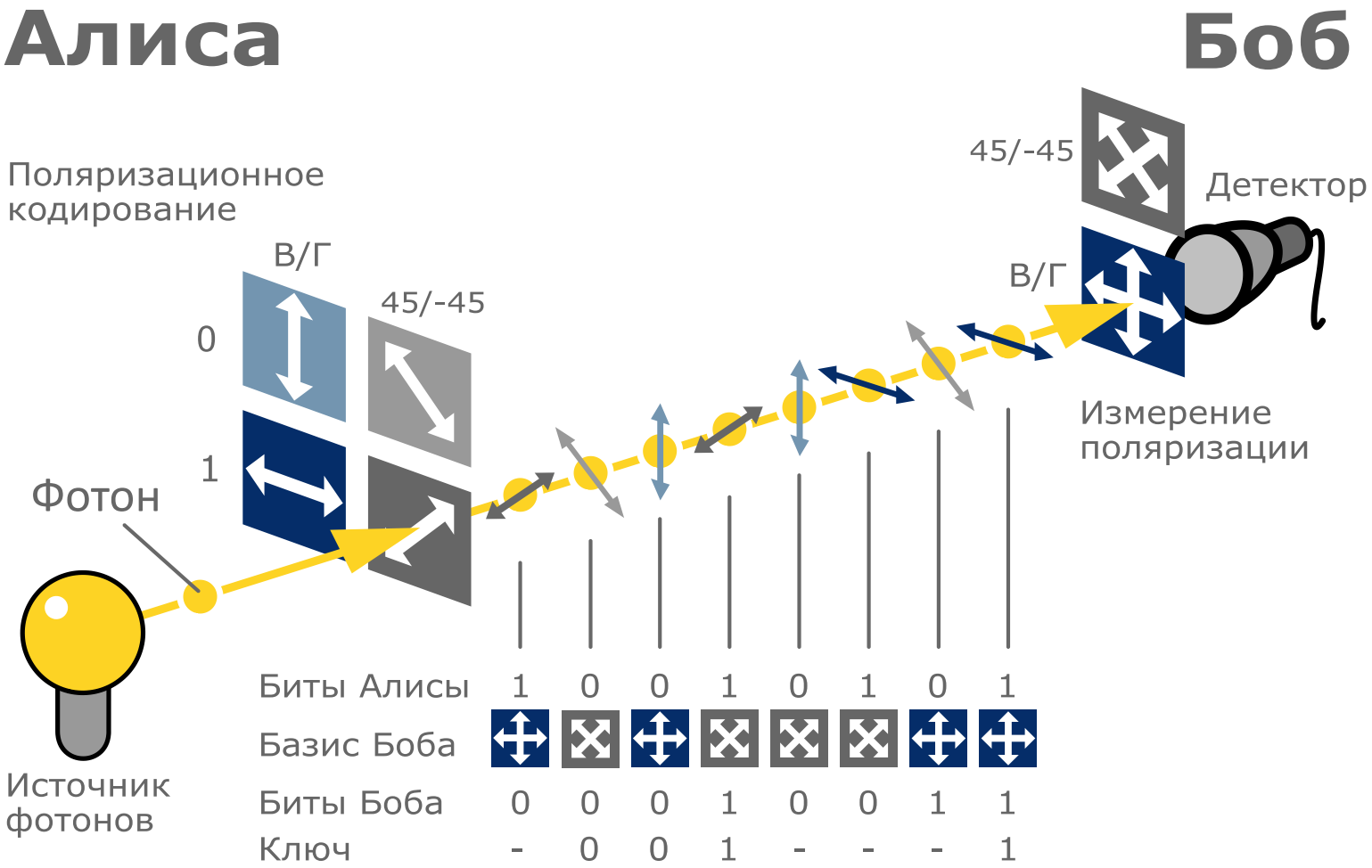
QKD: Генерация секретного ключа BB84

Алиса отправляет: -\-|/|\/
Боб выбирает: ++XXX+X+

Боб сообщает: ++XXX+X+
Алиса отвечает: +---+++-

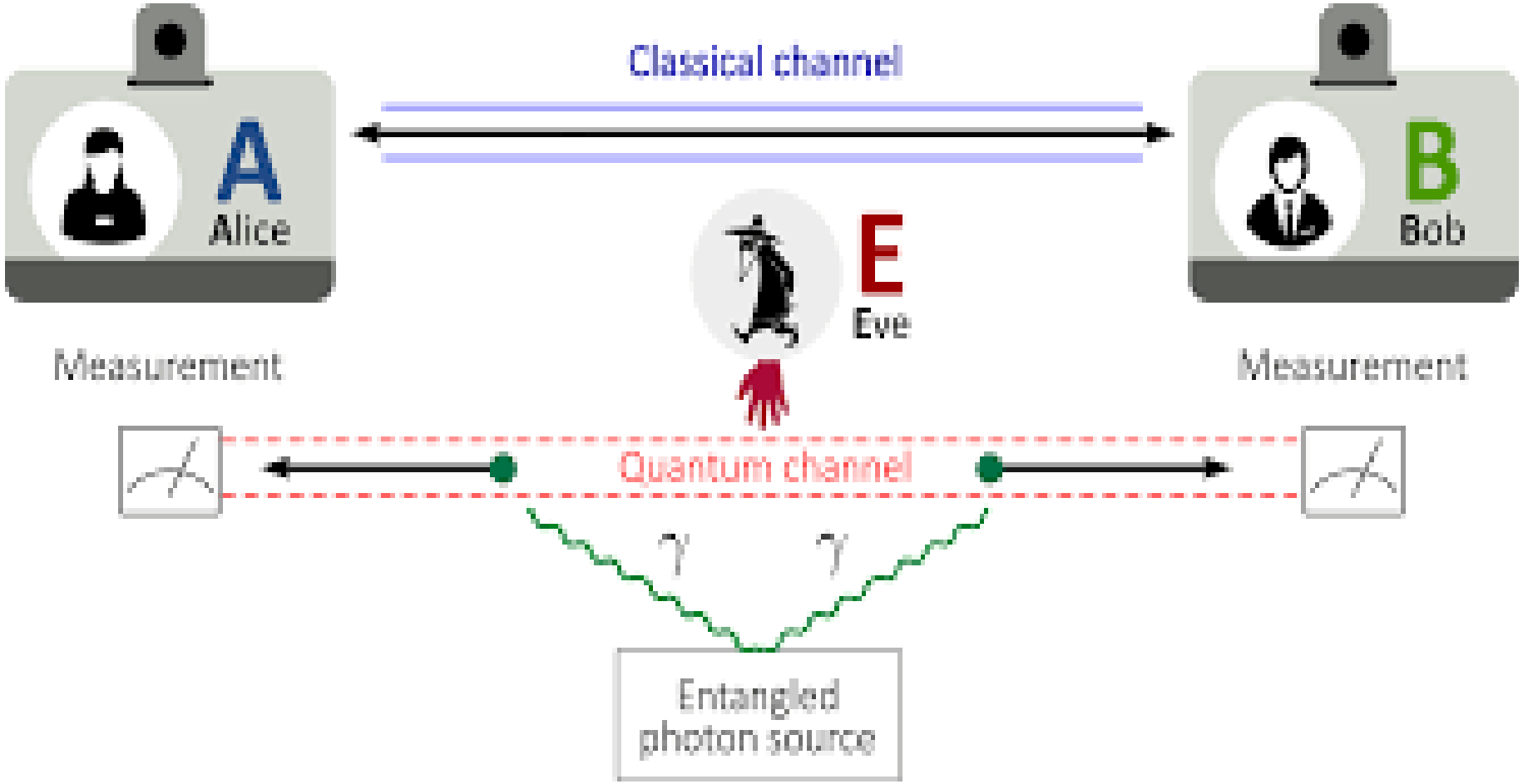
Оба отбрасывают случаи, где Боб не угадал.

Оба видят последовательность 1100



https://habrahabr.ru/post/315032/ *

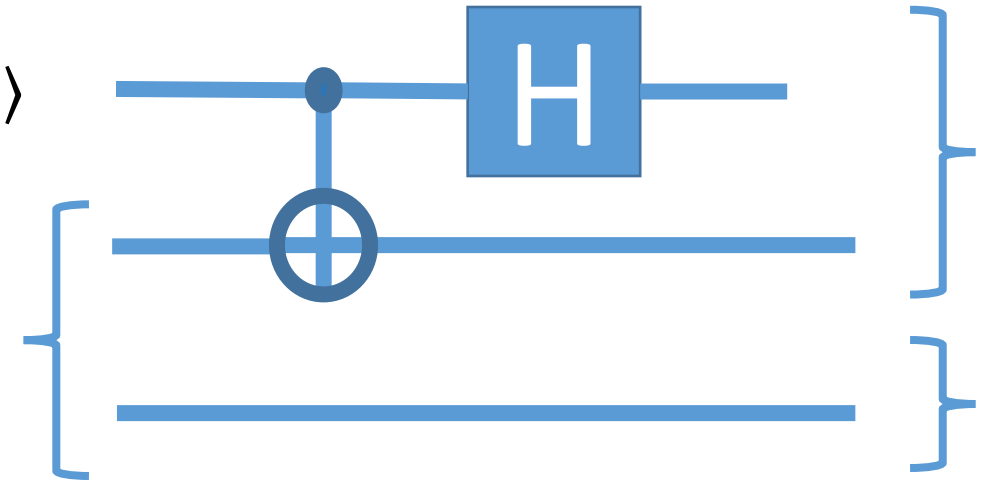
Обмен ключами. QKD: Алгоритм E91



Квантовая телепортация

$\alpha|0\rangle + \beta|1\rangle$

$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$



Кубиты Алисы

Кубит Боба

Хронология квантовых вычислений. До девяностых прошлого века

- **1973** — Александр Холево : n кубит не могут нести больше информации, чем такое же число классических битов (*теорема Холево*[en] или *ограничение Холево*). В этом же году Чарльз Х. Беннет показал возможность обратимости квантовых вычислений.
- **1975** — Р. П. Поплавский : «Термодинамические модели информационных процессов»(на русском), где показывает вычислительную невозможность симуляции квантовых систем на классических компьютерах из-за принципа суперпозиции.
- **1998** – первый работающий квантовый компьютер, 2 кубита
- **1976** — Польский физик и математик Роман Станислав Ингарден публикует работу под названием «Квантовая теория информации» в Reports on Mathematical Physics vol. 10, 43-72, 1976 (получена в 1975 году). Это одна из первых попыток создать квантовую теорию информации, так как Шеноном было показано, что классическая теория информации не может быть просто обобщена на квантовый случай. Но, тем не менее, такую теорию возможно построить так, чтобы она являлась некоторым обобщением шеноновской теории с учётом формализма квантовой механики и открытых систем и квантовых наблюдаемых.
- **1980** — Юрий Манин предложил идею квантовых вычислений.
- **1981** Ричард Фейнман в своей знаменитой лекции «Там внизу достаточно места» на Первой конференции по физике вычислений (MTI), отметил невозможность эффективно моделировать эволюцию квантовой системы на классическом компьютере, предложил базовую модель квантового компьютера, способного осуществить такое моделирование[2]. Томмазо Тоффоли[en] представил вентиль Тоффоли, который является популярным квантовым вентилем при построении обратимых схем квантовых компьютеров.
- **1982** Пауль Бениофф предложил первую теоретическую схему работы квантового компьютера[3]. Вуттерс и Зурек[4], а также независимо от них Диэкс[5] доказали теорему о запрете клонирования.
- **1984** Чарльз Беннетом и Жилем Брассард предложили первый протокол квантового распределения ключа — BB84.
- **1985** Дэвид Дойч впервые описал квантовую машину Тьюринга.

Хронология квантовых вычислений, девяностые

- **1991** Артур Экерт, Оксфордский университет - безопасная система связи на основе эффекта квантовой запутанности.
- **1993** Дэн Симон, Монреальский университет - метод вычисления с оракулом. В нем квантовый компьютер экспоненциально быстрее, чем обычный компьютер. В этом алгоритме - основные идеи, которые позже будут воплощены в квантовом алгоритме факторизации Питера Шора.
- **1994** Питер Шор, Лаборатория Белла, открыл важнейший квантовый алгоритм, позволяющий квантовым компьютерам быстро производить факторизацию больших целых чисел. Одновременно решены две важные задачи — проблема факторизации целых чисел и задача дискретного логарифмирования. Таким образом Алгоритм Шора теоретически позволяет взламывать используемые сейчас криптосистемы.
- **1995** Министерство обороны США организовало крупный семинар по вопросам квантовых вычислений и квантовой криптографии, где приняли участие ряд видных физиков США (Charles M. Bowden, Jonathan P. Dowling, и Henry O. Everitt). Питер Шор и Эндрю Штейн независимо друг от дуга предложили первую схему коррекции квантовых ошибок. Кристофер Монро и Дэвид Уайнленд впервые экспериментально реализовали процедуру контролируемого отрицания на основе пойманных в ловушку ионов по методике предложенной Сираком и Цоллером годом ранее.
- **1996** Квантовый алгоритм поиска в базе данных (Лов Гровер из «Лаборатории Белла») позволяет добиться квадратичного прироста скорости расчетов по сравнению с обычным компьютером и может быть применен к гораздо более широкому спектру задач. Любая задача, которую можно свести к неинформированному методу поиска (полный перебор), также будет иметь квадратичный прирост скорости. Дэвид П. ДиВинсензо из IBM, предложил перечень минимальных требований необходимых для создания квантового компьютера.

Хронология квантовых вычислений. 1997-1999

- **1997** Дэвид Кори, Арм Фахми и Тимоти Хавел, одновременно с ними Нил Гершенфельд и Исаак Чанг из MIT опубликовали работы, впервые описывающие возможность практически реализовать квантовый компьютер на основе эффекта объемного спинового резонанса или тепловых ансамблей. Эта технология основана на явлении ядерного магнитного резонанса (ЯМР), явлении которое так же нашло применение в медицине подарив человечеству устройства магнитно-резонансной томографии. Алексей Китаев описал принципы топологических квантовых вычислений как метод борьбы с декогеренцией. Дениел Лосс и Дэвид П. ДиВинсензо предложили квантовый компьютер Лосса-ДиВинсензо[en], использующий в качестве кубитов собственный момент импульса отдельно взятых электронов, запертых в квантовых точках.

- **1998.** Сэмюэл Л. Браунштейн и его коллеги показали, что ни в каком ЯМР-эксперименте смешанного состояния квантовой запутанности не существует. Но смешанное состояние квантовой запутанности является необходимым условием для квантового ускорения вычислений. “Это стало доказательством того, что ЯМР-компьютеры не имеют ни какого преимущества по сравнению с обычными компьютерами.

Хронология квантовых вычислений. Двухтысячные

- **2000**
  - Первый работающий пяти кубитный ЯМР-компьютер был продемонстрирован в Мюнхенском техническом университете.
  - Первое выполнение нахождения порядка (что является важной частью алгоритма Шора) продемонстрировано в исследовательском центре компании IBM и в Стэнфордском университете.
  - Первый работающий семи кубитный ЯМР-компьютер был продемонстрирован в Лос-Аламосской национальной лаборатории
  - 5- и 7-кубит компьютеры
- **2001** Первое полное выполнение алгоритма Шора продемонстрировано в исследовательском центре компании IBM и в Стэнфордском университете. Число 15 было факторизованно квантовым компьютером, используя массив из 10^{18} идентичных молекул, каждая из которых содержала семь активных ядерных спинов.
- **2006** – 12-кубит компьютер
- **2007** – 28-кубит компьютер
- **2012** – 84-кубит компьютер

Хронология квантовых вычислений. 2015-2016

- **2015**
  - Оптически адресуемые ядерные спины в твердом теле с временем когерентности сохраняющимся на протяжении 6 часов.[6]
  - Квантовая информация была закодирована простыми электрическими импульсами.[7]
  - Написан код для обнаружения квантовых ошибок с использованием квадратной решетки из четырёх сверхпроводящих кубитов.[8]
  - Разработан двухкубитный логический вентиль из кремния.[9]
  - 1000-кубит компьютер
- **2016**
  - Google, используя массив из 9 сверхпроводящих кубитов, разработанных группой Martinis и Калифорнийским университетом в Санта-Барбаре, смоделировали молекулу водорода.[10] **2016** – Google разрабатывает quantum computer

Хронология квантовых вычислений. 2017-2018

- **2017**
  - Microsoft представила язык квантового программирования интегрированный в Visual Studio. Программы могут выполняться либо на симуляторе 32-кубитного компьютера локально, либо на симуляторе 32-кубитного компьютера в облаке Microsoft Azure.[11]
  - Ученые создали микрочип, который генерирует два запутанных кубита, с 10 различными состояниями, для 100 измерений в общем.[12]
  - В Intel разработана 17-кубитная микросхема.[13]
  - 2048-кубит компьютер. IBM, Microsoft, аннонсируют квантовые компьютеры
- **2018** – Появляются несколько quantum microprocessors

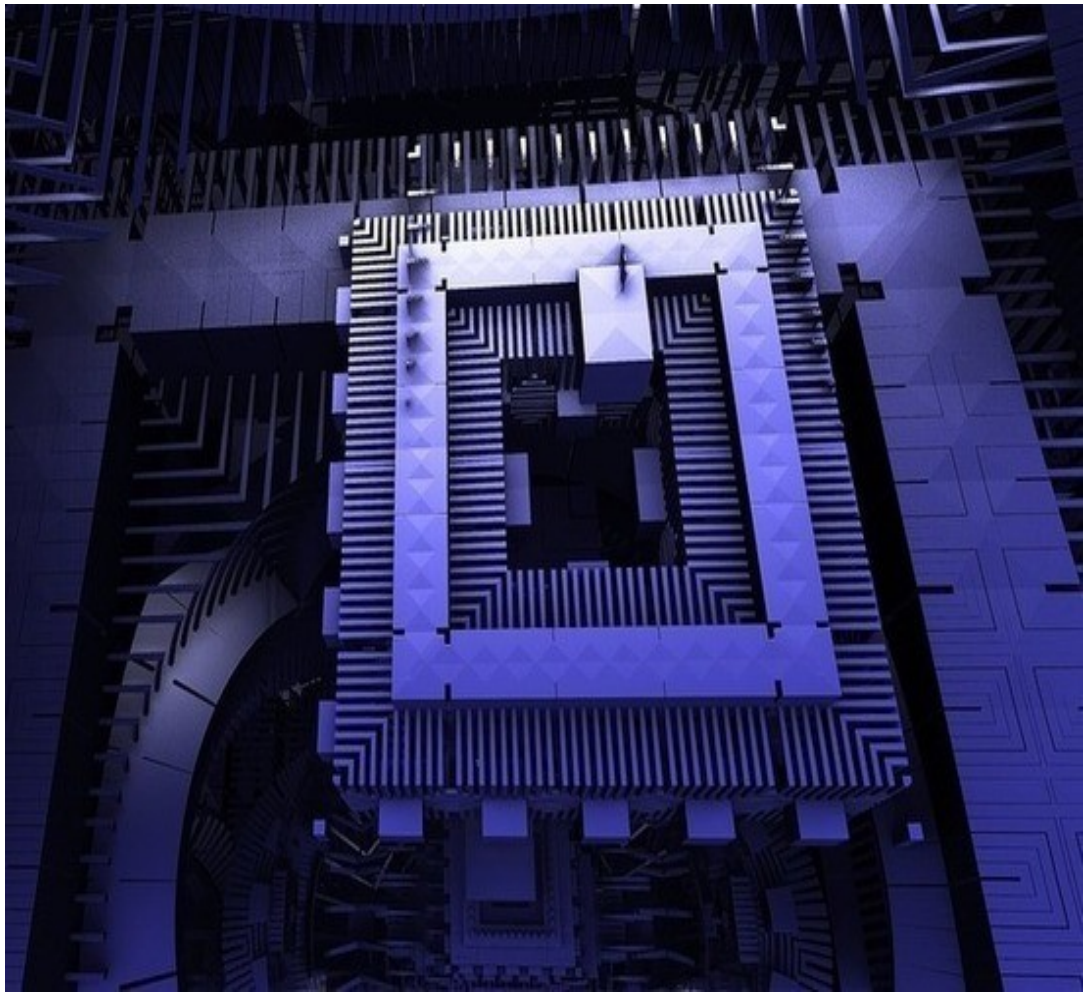
Хронология квантовых вычислений. 2019

Госкорпорация «Росатом» объявила о запуске проекта по созданию отечественного квантового компьютера, который поможет России войти в число стран-лидеров «квантовой гонки». К 2024 году десятилетнее отставание России по квантовым технологиям хотят сократить до двух-трех лет.

Госкорпорация «Росатом» запускает проект по созданию российского квантового компьютера, говорится в поступившем в Forbes сообщении компании.

Проект рассчитан на срок до 2024 года, его финансирование составит 24 млрд рублей. Из этой суммы 13,3 млрд рублей — бюджетные средства, а остальное — инвестиции «Росатома» и других компаний, которые будут участвовать в реализации проекта.

Хронология квантовых вычислений. 2019+



Проект «Росатом» рассчитан на срок до 2024 года, его финансирование составит 24 млрд рублей.

Из этой суммы 13,3 млрд рублей — бюджетные средства. Остальное — инвестиции «Росатома» и др. компаний, они будут участвовать в реализации проекта.
Сейчас под эгидой Росатома разработкой квантовых вычислителей занимается ВНИИА им. Духова.

Над созданием элементов квантового компьютера – кубитпроектом работают также ученые МГУ, МФТИ, НИТУ «МИСиС», НОЦ ФМН, ФИАН, Российского квантового центра и ряда академических институтов. Однако пока российским специалистам не удалось создать системы, состоящие более чем из двух кубитов, а американские и европейские ученые демонстрируют устройства, построенные на 50-70 кубитах.

https://www.mk.ru/science/2019/11/07/rosatom-zayavil-o-sozdanii-rossiyskogo-kvantovogo-kompyutera-k-2024-godu.html

Применение квантовых компьютеров на практике

В квантовые компьютеры инвестируют миллиарды долларов в надежде, что однажды они изменят мир. Однако это «однажды» все не наступает. Российский физик Михаил Дьяконов, ведущий исследования в лаборатории Шарля Кулона Университета Монпелье (Франция), считает, что многообещающее направление науки превращается в пиар-пузырь и скоро интерес к нему угаснет.*

«Проблема кадров не решается, даже если завтра нам дать миллиард»**

https://hightech.plus/2018/11/24/fizik-mihail-dyakonov-kvantovii-kompyuter-dlya-prakticheskogo-primeneniya-nevozmozhen *

https://hightech.plus/2018/11/02/kvantovoe-prevoshodstvo-mozhet-bit-dostignuto-hot-v-etom-godu **