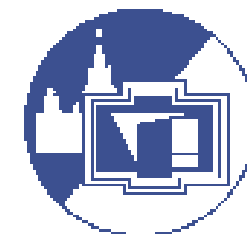


Ежегодная международная научно-практическая конференция  
«РусКрипто'2021»

# Квантовые вычисления в России и мире



**Сергей Кулик,**

Профессор, научный руководитель Центра квантовых технологий физического факультета МГУ имени М.В.Ломоносова

## Вместо предисловия



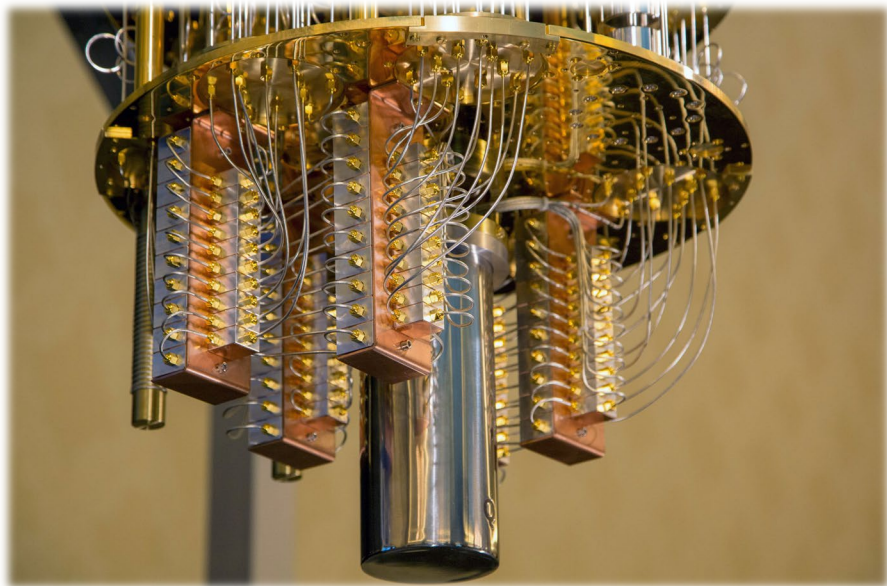
**“Думаю, я с уверенностью могу  
сказать, что никто не понимает  
квантовую механику”**

*Ричард Фейнман,  
Лауреат Нобелевской  
премии по физике 1965 года.*

# Что такое квантовый компьютер?

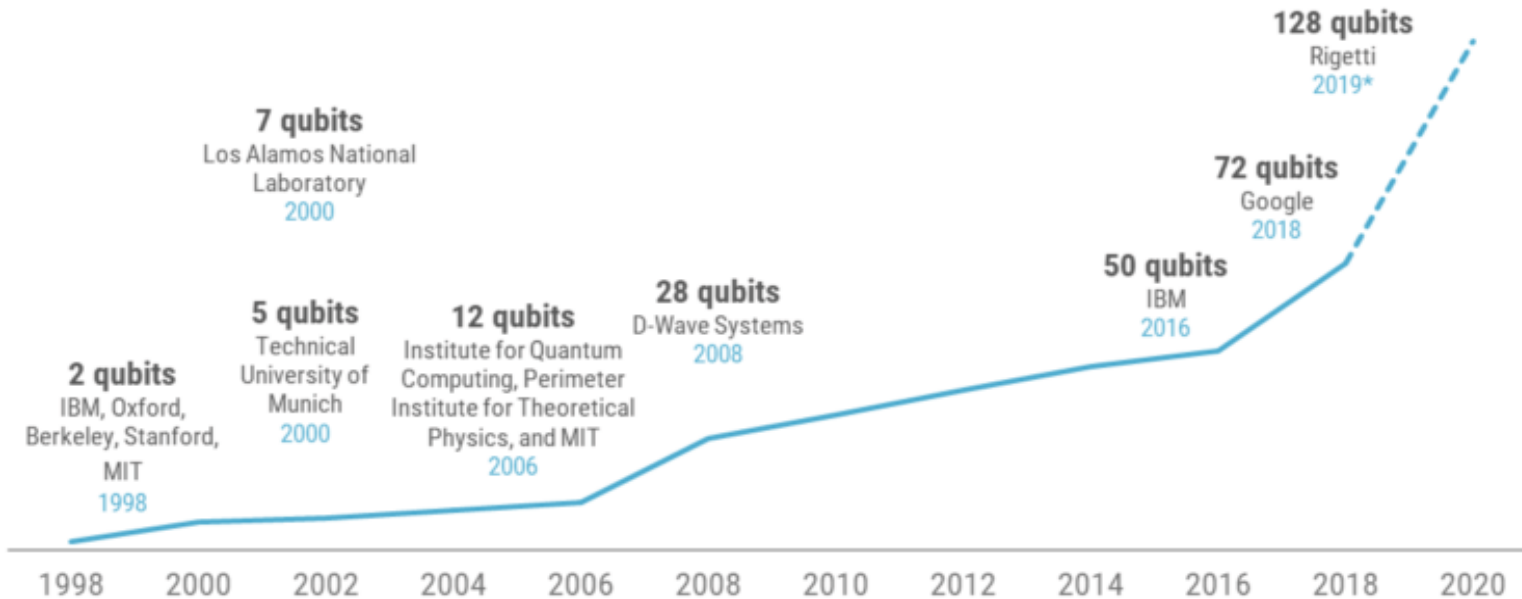
- Это физическое устройство, выполняющее логические операции над квантовыми состояниями путем унитарных преобразований (т.е. сохраняющих энергию), не нарушающих квантовые суперпозиции в процессе вычислений.
- **Проблема 1** - уменьшение размеров интегральных схем, т.е. отдельных элементов. Нанотехнологии. Естественный предел здесь - характерный масштаб атома, когда вступают в силу законы микромира, т.е. квантовой механики.
- **Проблема 2** – уменьшение доли рассеиваемой энергии. Логически обратимые операции - те, которые не сопровождаются рассеянием энергии (Ландауэр, 1961г.).

# ПРОГРЕСС В ОБЛАСТИ КВАНТОВЫХ ВЫЧИСЛЕНИЙ



## Quantum computers are getting more powerful

Number of qubits achieved by date and organization 1998 – 2020\*

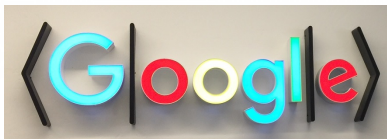


Source: MIT, Qubit Counter. \*Rigetti quantum computer expected by late 2019.

# ПРИЛОЖЕНИЯ КВАНТОВЫХ АЛГОРИТМОВ

IT гиганты

IBM Q™



Microsoft  
Технологический



\$210M



\$119M



## In Russia

Центры НТИ



МИСиС

Другие большие проекты




Основное внимание:  
разработка «железа»

Source: cbinsights.com

Стартапы

1QBit



XANADU



CAMBRIDGE QUANTUM COMPUTING



QCWARE



ZAPATA



quantumbenchmark



RQuanTech

Boosting the Qubit Revolution

Индустрия квантовых компьютеров –  
быстро развивающаяся отрасль

# СПЕЦИАЛИЗИРОВАННЫЙ КВАНТОВЫЙ СОПРОЦЕССОР



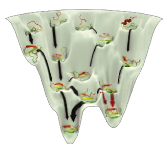
## Квантовый отжиг



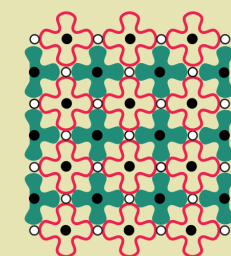
**ПРИМЕНЕНИЕ**  
глобальная оптимизация

**УНИВЕРСАЛЬНОСТЬ**  
ограниченная

**ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ**  
ограниченная



## КЛАССИЧЕСКИЙ ВЫЧИСЛИТЕЛЬНЫЙ КЛАСТЕР



## КВАНТОВЫЙ СОПРОЦЕССОР

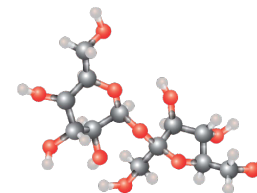
## NISQ устройство

**ПРИМЕНЕНИЕ**  
квантовая химия  
наука о материалах  
глобальная оптимизация  
задачи сэмплинга  
квантовая динамика



**УНИВЕРСАЛЬНОСТЬ**  
частичная

**ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ**  
высокая?



## Универсальный квантовый компьютер



**ПРИМЕНЕНИЕ**  
защищенные вычисления  
машинное обучение  
криптография  
квантовая химия  
наука о материалах  
глобальная оптимизация  
задачи сэмплинга  
квантовая динамика  
задачи поиска

**УНИВЕРСАЛЬНОСТЬ**  
полная, математически обоснованное  
ускорение

**ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ**  
очень высокая

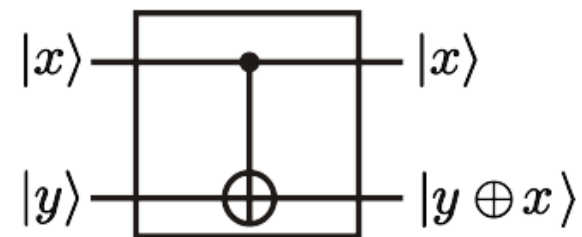
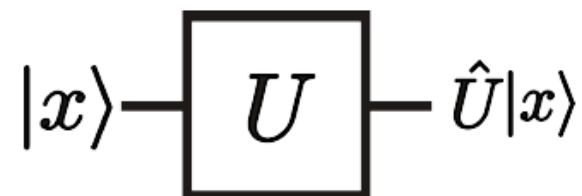


Сегодня обозначена возможность  
использования квантового компьютера для  
решения практически значимых задач

# КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

- ▶ Произвольные однокубитные преобразования
- ▶ Перепутывающие двухкубитные преобразования, например CNOT

Универсальный набор гейтов <sup>1</sup>



<sup>1</sup>A. Barenco, *et al.*, Elementary gates for quantum computation, Phys. Rev. A **52**, 3457 (1995)

# КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: критерии

## Критерии Ди Винченцо:

- масштабируемость;
- надежная инициализация;
- **большие времена декогеренции (релаксации)**  
**по сравнению с временем срабатывания**  
**отдельных гейтов;**
- возможность манипуляций;
- передача и считывание состояний кубитов,

-



# КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: платформы

Сегодня имеется несколько физических платформ для реализации квантовых вычисл  
Ни одна из этих платформ не удовлетворяет в полной мере этим критериям



P.N. Lebedev  
Physical Institute



1. Ядерный магнитный резонанс

2. Ионы в ловушках

3. Нейтральные атомы в микродипольных ловушках

4. Квантовая электродинамика резонаторов

5. Линейные (и нелинейно) оптические вычисления (фотонные чипы)

6. Твердотельные системы на основе квантовых точек

7. Сверхпроводниковые цепи

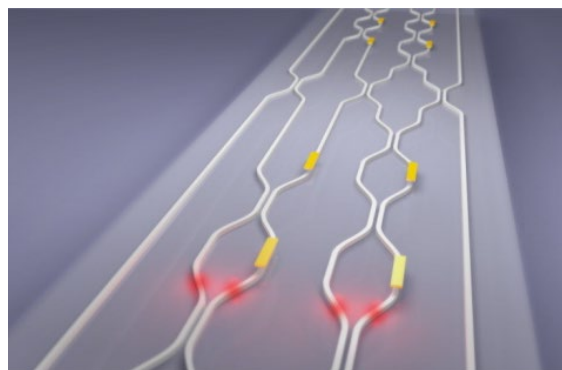


8. Твердотельные системы на основе спинов

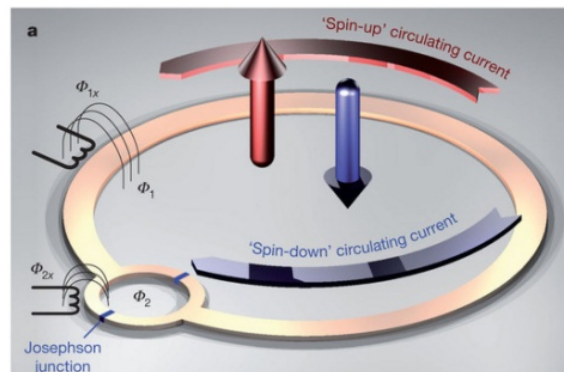
9. Биологические и высокомолекулярные системы



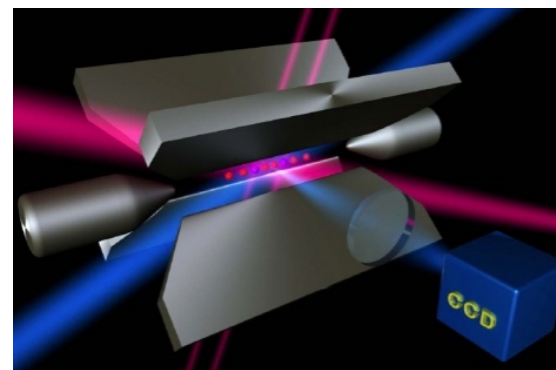
# Варианты физических моделей



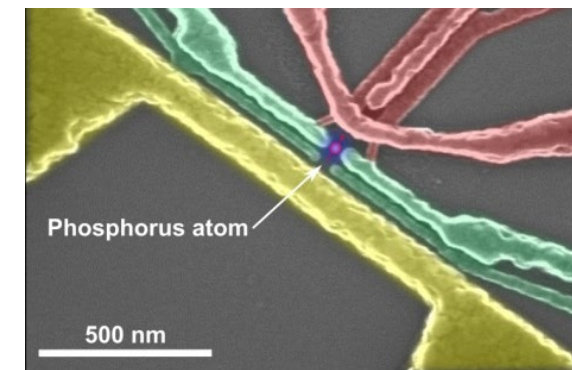
Оптические  
интегральные схемы



Сверхпроводящие  
цепи

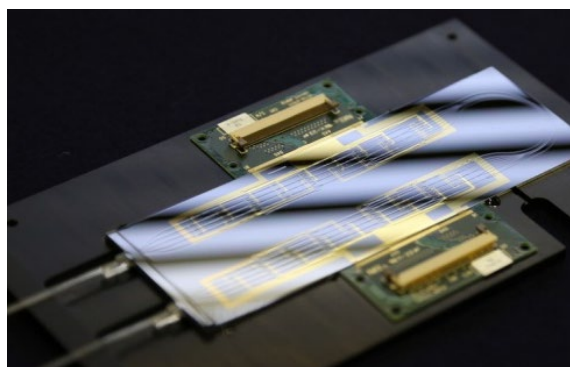


Ионы/атомы  
в ловушках

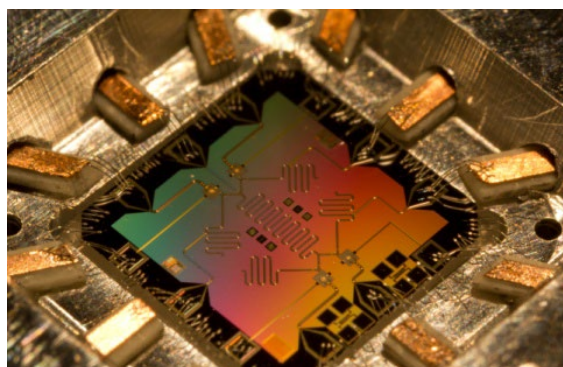


Квантовые точки  
/примесные атомы

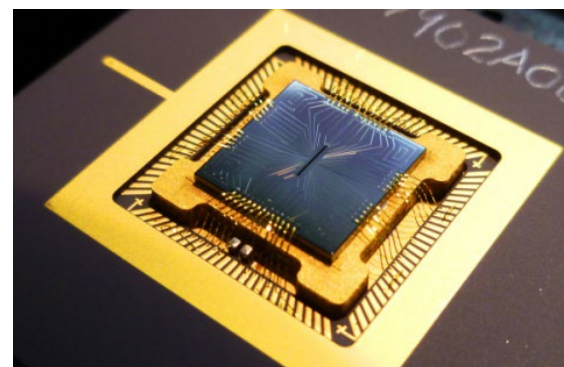
# Современное состояние технологии



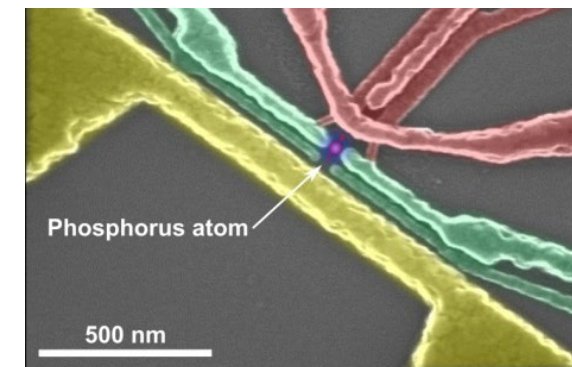
Оптические  
интегральные схемы



Сверхпроводящие  
цепи



Ионы/атомы  
в ловушках



Квантовые точки  
/примесные атомы

# Перспективные физические системы для построения полномасштабных квантовых компьютеров

1 – Ионы в ловушках; 2 – Нейтральные атомы; 3 – Сверхпроводниковые цепи;  
 4 – Примесные спины; 5 – Полупроводниковые структуры;  
 6 – Биологические системы; 7 – фотонные чипы.




КРИТЕРИИ	1	2	3	4	5	6	7
	Оценка (пятибальная шкала)						
Масштабируемость	3	4	4	3,5	2	4	3/5+
Возможность инициализации	5	4	4.5	4.5	5	5	5
Большие времена когерентности (много больше, чем длительность одной операции)	4,5	4,5	3	5	3	?	4
Реализация универсального набора гейтов	5	3	4	4	4	3	5(1)/3(2)
Возможность измерения отдельных кубитов	5	4,5	4,5	4,5	4	2	4

# КОЛИЧЕСТВЕННОЕ СРАВНЕНИЕ

	Ионы	Нейтральные атомы	Сверхпроводники	ФОТОНЫ
Масштабируемость	Симуляторы - <b>53</b> кубита <b>1D-2D</b> Вычислители - <b>11</b> кубит (попарно связанных) [1,2]	Симуляторы – <b>51</b> кубит <b>1D-3D</b> [5]	Вычислители - <b>72</b> кубита <b>1D-2D</b> [9]	100 кубитов
Время когерентности	До <b>10 мин</b> [3]	До <b>7 с</b> [6]	До <b>320 мкс</b> [10]	бесконечное
Время гейта	От <b>1 мкс</b>	<b>400 нс</b>	<b>10 нс</b>	менее 1нс
Fidelity	<b>99.996%</b> один кубит [4] <b>99.9%</b> два кубита [4]	<b>99.6%</b> один кубит [7] <b>97.4%</b> два кубита [8]	<b>99.92 %</b> один кубит[11] <b>99.4%</b> два кубита [11]	<b>99,9</b> один кубит <b>99,9</b> два кубита*
Отношение времени когерентности к времени гейта	До <b>10<sup>9</sup></b>	До <b>10<sup>7</sup></b>	До <b>10<sup>4</sup></b>	бесконечное

\* Вероятностная модель – 10%

# ПРОГНОЗИРУЕМЫЕ ФАЗЫ ЗРЕЛОСТИ КВ\*

	NISQ era 3–5 years	Broad quantum advantage 10+ years	Full-scale fault tolerance 20+ years
 Technical achievement	Error mitigation	Error correction	Modular architecture
 Example of business impact	Material simulations that reduce expensive and time-consuming trial-and-error lab testing	Near-real-time risk assessment for financial services firms (e.g., quant hedge funds)	De novo drug design with large biologics that have minimal off-target effects
 Estimated impact (operating income)	\$2 billion–\$5 billion	\$25 billion–\$50 billion	\$450 billion–\$850 billion

\* According to Boston Consulting Group report

# ПЕРСПЕКТИВНЫЕ ЗАДАЧИ ДЛЯ КВ\*

Задача	Полезно для...	Отраслевые приложения
Комбинаторная оптимизация	Минимизация или максимизация целевой функции, например, поиск наиболее эффективных ресурсов или поиск самого короткого расстояния между точками (задача странствующего коммивояжера)	<ul style="list-style-type: none"> <li>• Оптимизация сети (например, для авиалиний, такси)</li> <li>• Оптимизация цепочек поставок и/или логистики</li> <li>• Оптимизация финансовых сервисов</li> </ul>
Решение систем дифференциальных уравнений	Моделирование поведения сложных систем, (например, уравнение Навье-Стокса в гидродинамике)	<ul style="list-style-type: none"> <li>• Моделирование гидродинамики для дизайна - автомобильной и авиационной техники;</li> <li>• Моделирование медицинских приложений (например, анализ кровотока);</li> <li>• Молекулярное моделирование новых материалов и/или лекарств</li> </ul>
Решение систем линейных уравнений	Задачи машинного обучения с использованием матрицы диагонализации (например в задаче кластеризации)	<ul style="list-style-type: none"> <li>• Управление рисками в финансовой сфере</li> <li>• Классификация последовательностей ДНК</li> <li>• Маркетинг и сегментация клиентов</li> </ul>
Задача факторизации	Криптография и компьютерная безопасность, (например, RSA)	<ul style="list-style-type: none"> <li>• Дешифрование и/или взлом кода</li> </ul>

# Преимущества атомной архитектуры

## Масштабируемость массива

- Современный уровень  $\sim 100$  атомов
- Перспектива  $\sim 10^4$  (мощность лазера  $\sim 10$  Вт)
- С учётом потерь атомов  $\sim 2000$  физических кубитов

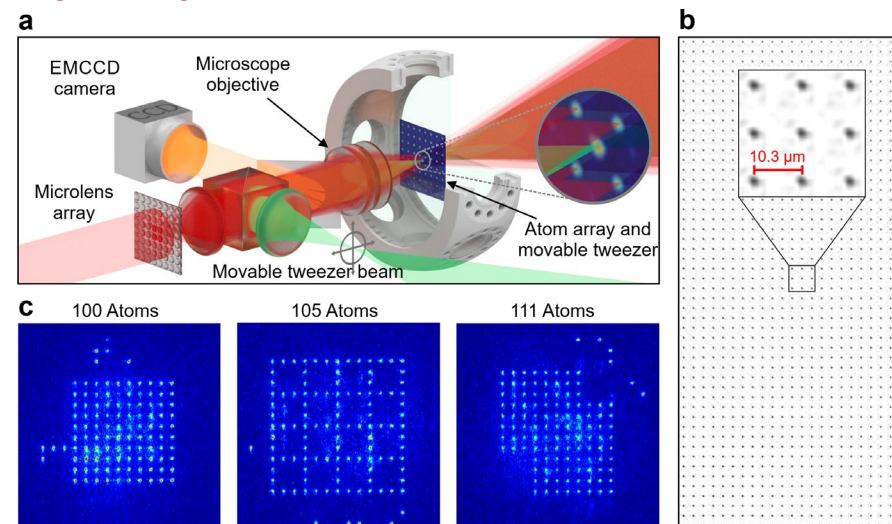
## Высокая связность кубитов

- 2D и 3D массивы
- Связь не ограничена ближайшими соседями
- Все атомы внутри радиуса блокады могут быть запутаны за один такт
- **Нативные многокубитные гейты**

## Большие времена когерентности

- Время когерентности в микроловушке  $\sim 1$  с
- Ошибки однокубитных вентилей  $< 10^{-4}$
- Ошибки двухкубитных вентилей  $< 3\%$

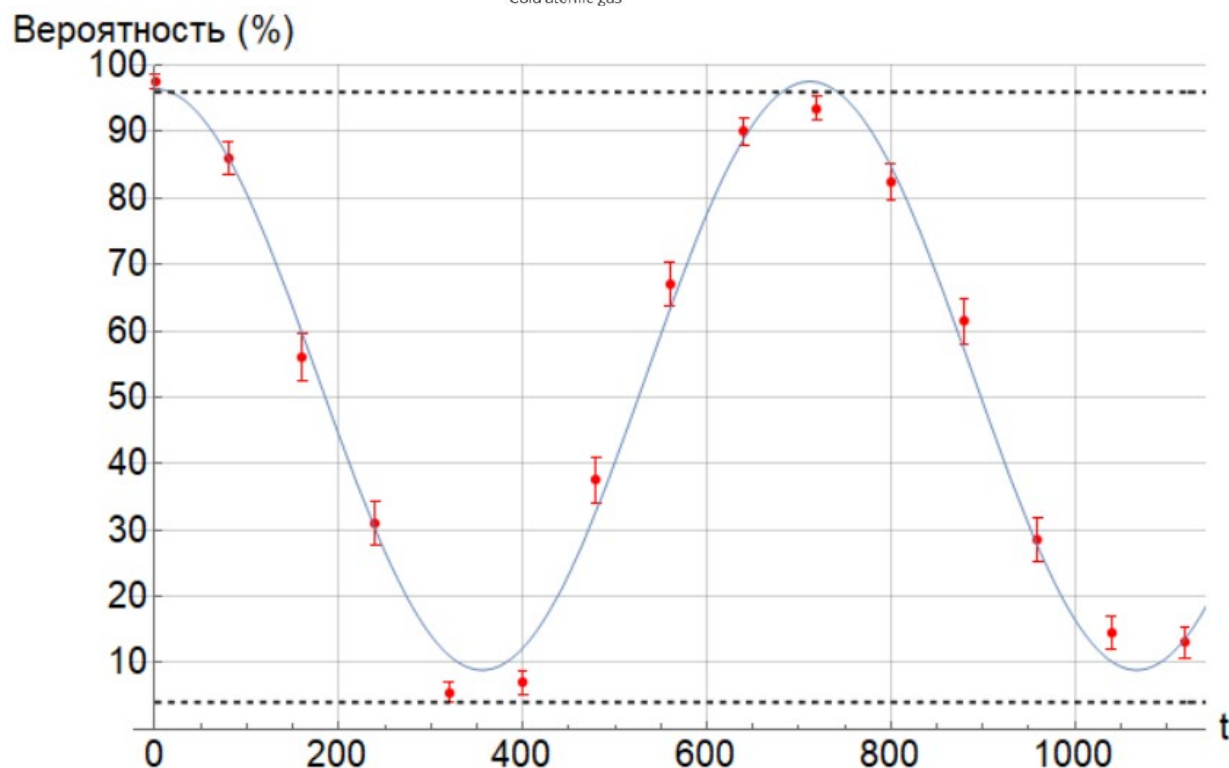
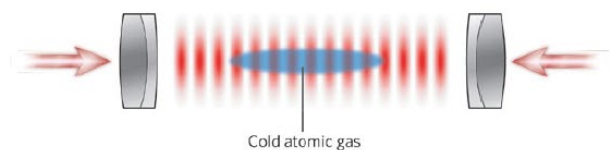
## Переключение в режим аналогового симулятора без изменений в «железе»



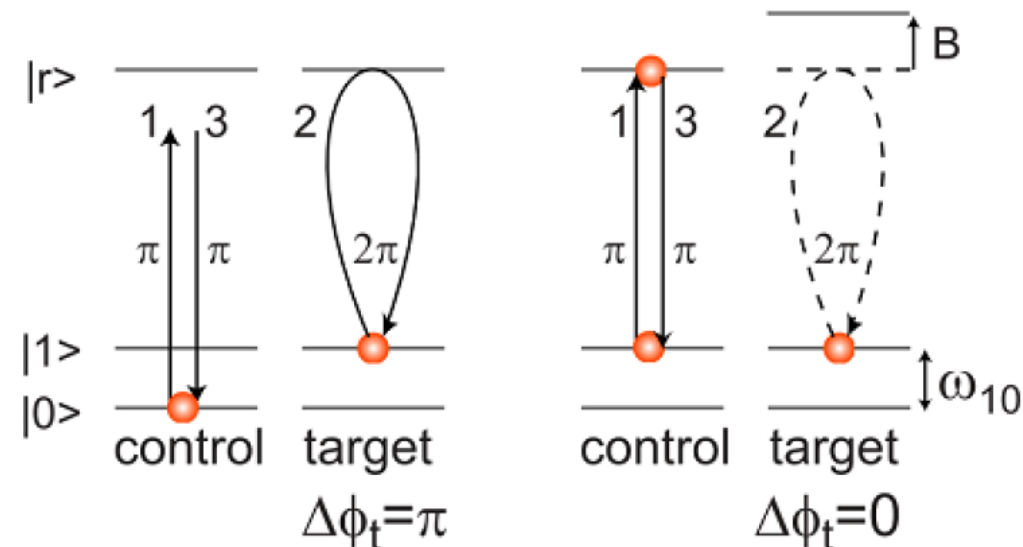


# ВЫЧИСЛЕНИЯ НА НЕЙТРАЛЬНЫХ АТОМАХ: гейты

Однокубитный гейт

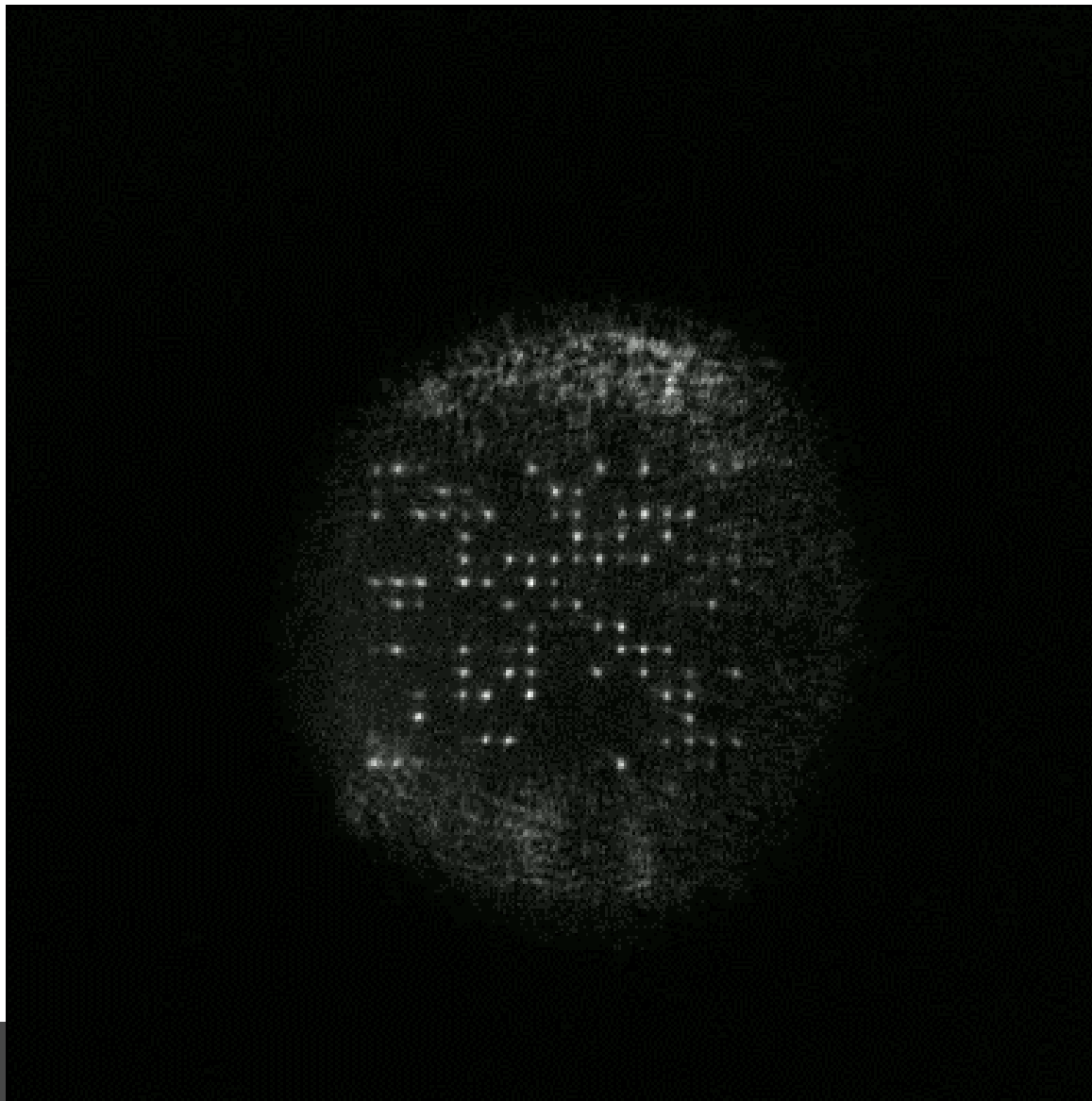


Двухкубитный гейт: CZ. Ридберговская блокада

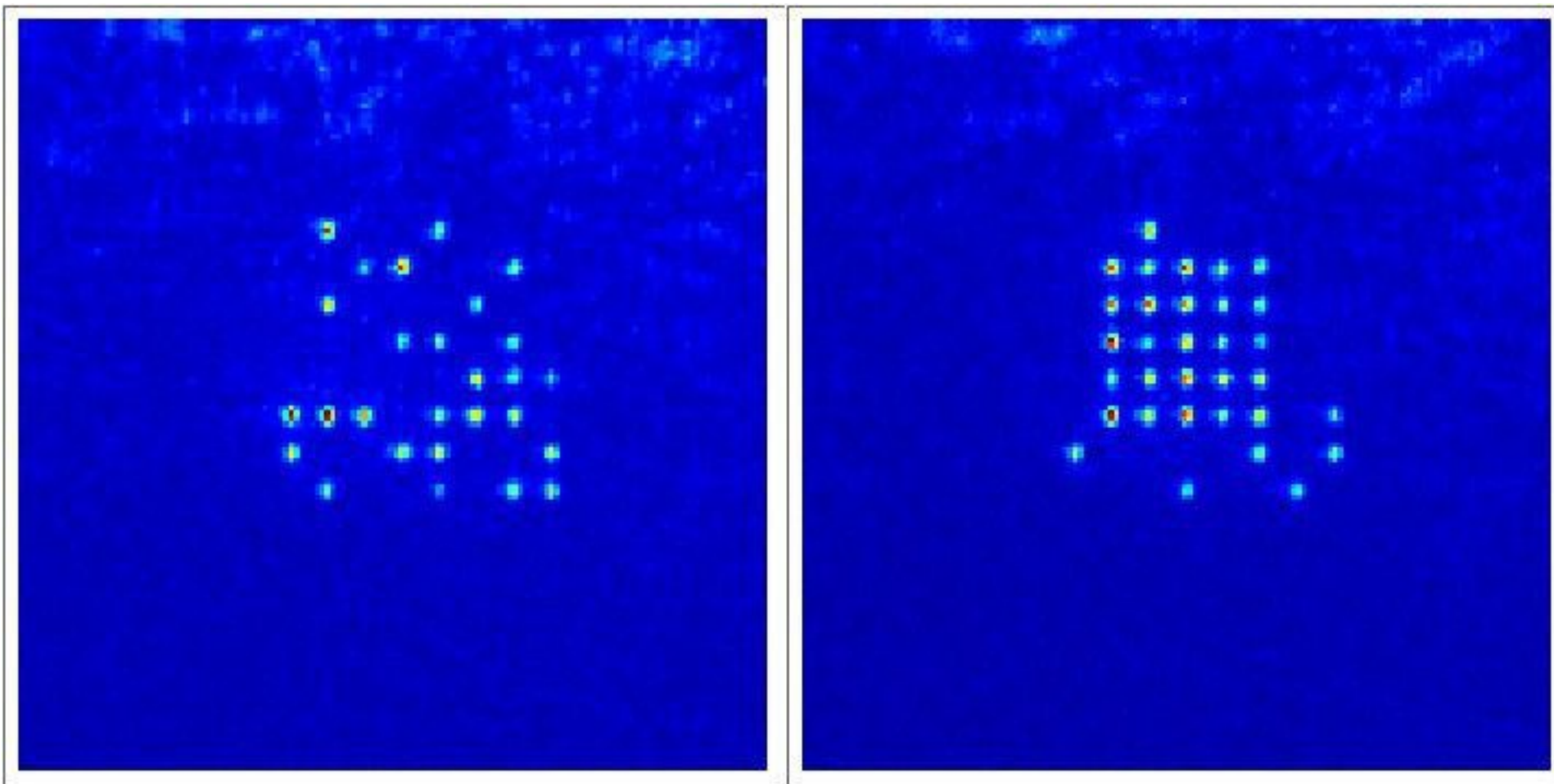


[Jaksch et al. PRL, 85, 2208 (2000)]

# Регистр из 121 атомов: реальное время



# Атомные регистры: однородное заполнение



# Линейно-оптические вычисления: преимущества\*

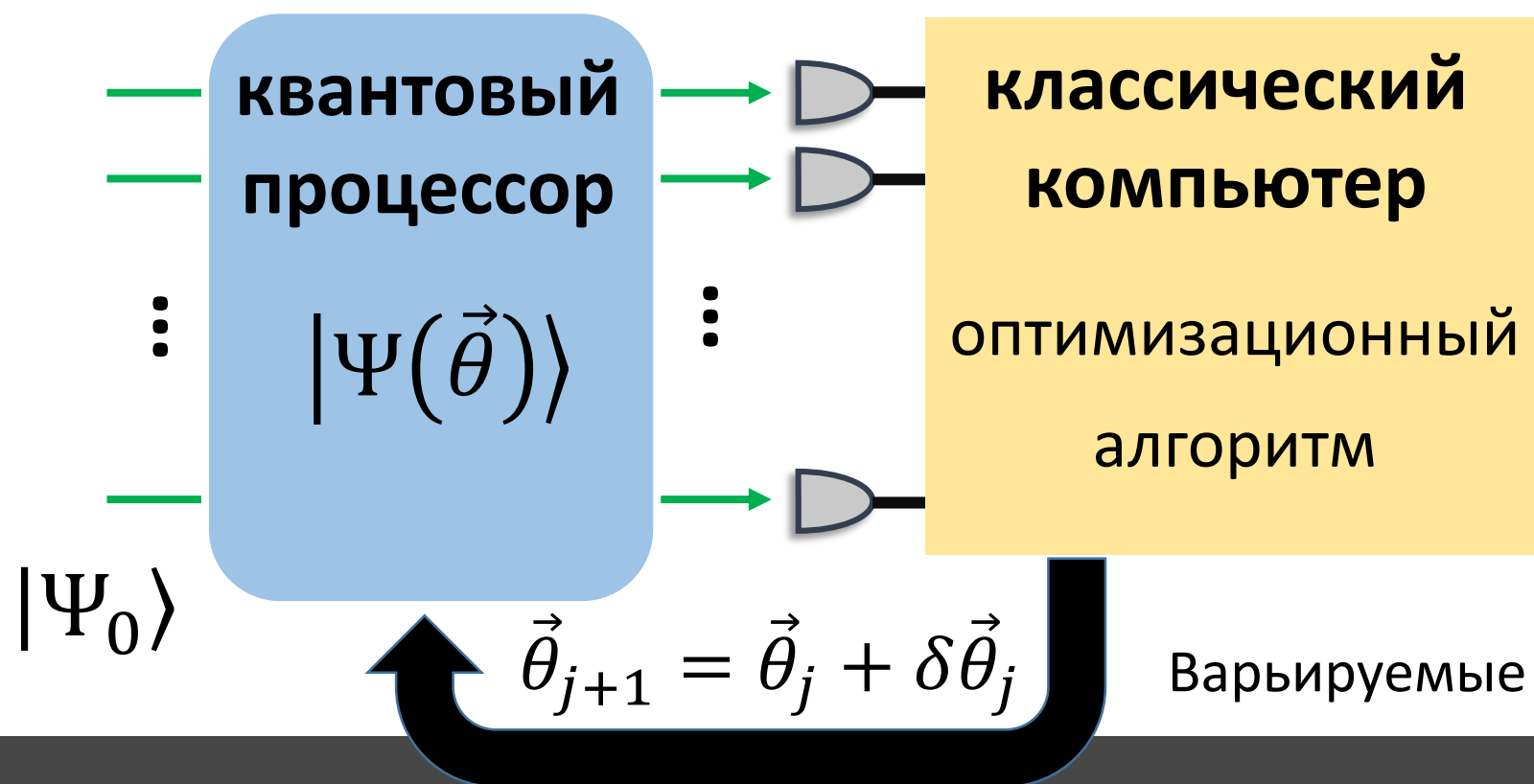
1. Фотоны – быстрые (“Flying qubits”);
2. Фотоны – дешевые;
3. Низкие значения нелинейных восприимчивостей – фотоны плохо взаимодействуют с окружением;
4. Аппаратная и технологическая часть хорошо развита – технология телекоммуникаций, интегральная оптика;
5. Естественная платформа для некоторых квантовых алгоритмов (Quantum Walks, Boson Sampling)

«Люди, не имеющие недостатков, имеют, как правило, мало достоинств». *Авраам Линкольн*

# Линейно-оптические вычисления: вариационный алгоритм (VQE)

измерения кубитов

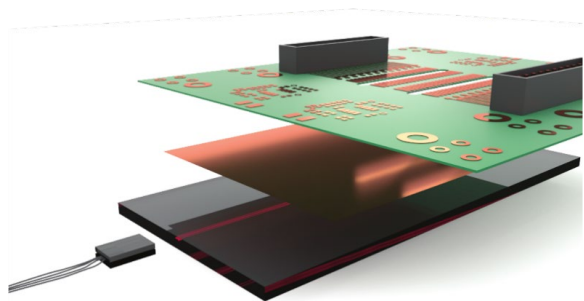
Глобальный минимума гамильтониана:



$$E(\vec{\theta}) = \frac{\langle \Psi(\vec{\theta}) | \hat{H} | \Psi(\vec{\theta}) \rangle}{\langle \Psi(\vec{\theta}) | \Psi(\vec{\theta}) \rangle},$$

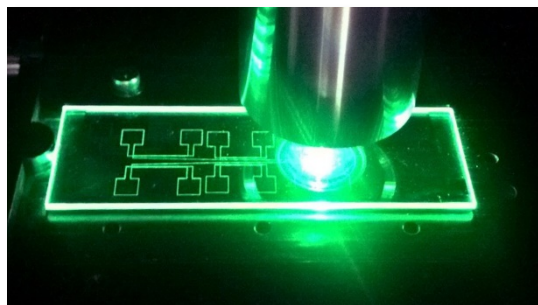
Варьируемые параметры:  $\vec{\theta} = (\theta_1, \dots, \theta_P)$

# Технологическая база



## Фемтосекундная лазерная печать

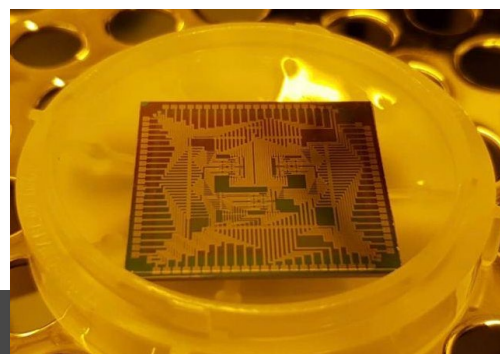
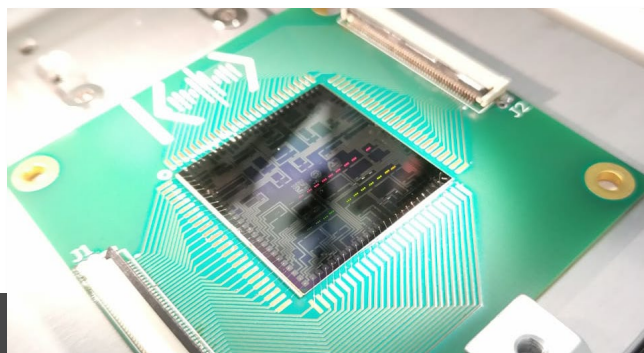
- Оптические потери менее 1 дБ/см
- Термооптические фазовращатели
- Время переключения 10 мс
- Ошибка приготовления  $10^{-3} - 10^{-2}$
- Продвинутое управление



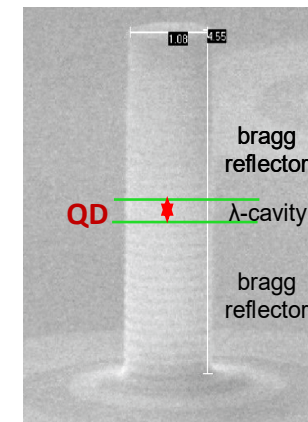
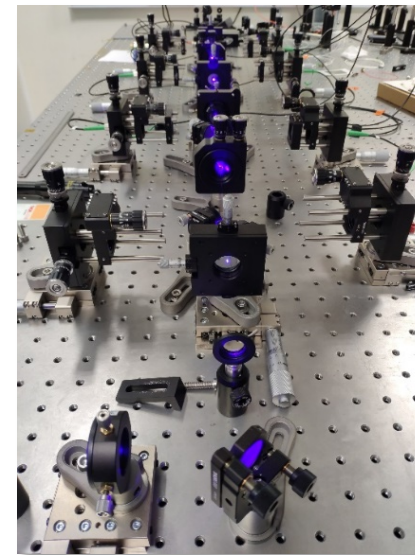
## SiN волноводы (совместно с МГТУ)

- Оптические потери менее 1 dB/cm
- Термооптические фазовращатели
- Компактные размеры
- Схемы большого масштаба

## Последнее поколение чипов НОЦ ФНМ МГТУ:



# Многофотонные источники



Однофотонный источник  
ФТИ им. Иоффе

## На основе СПР

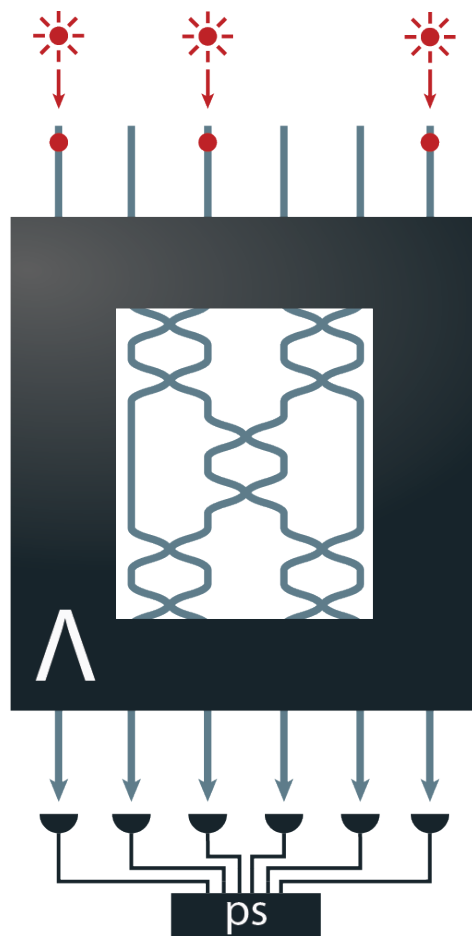
- До 6 фотонов
- Неразличимость 0.99
- Скорость генерации 6 фотонов  $\sim 10$  Гц

## На квантовых точках

- Высокая яркость
- Неразличимость
- 10 канальный демультиплексор

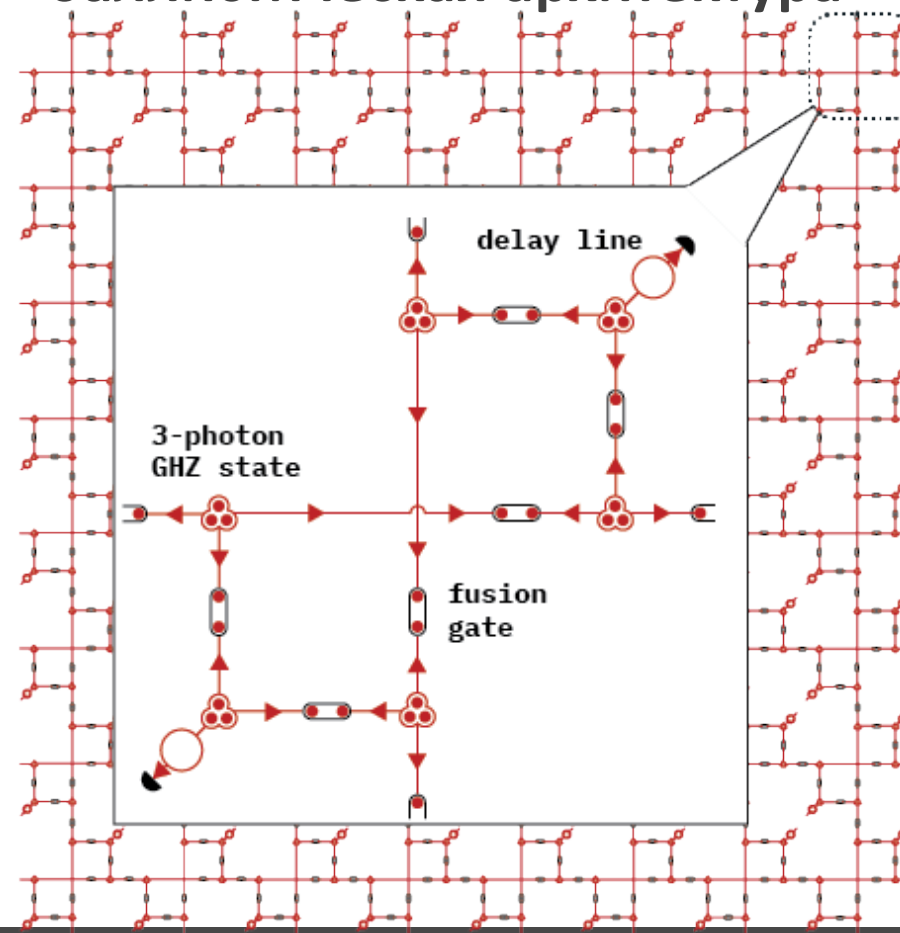
# Линейно-оптические вычисления

Ближнесрочная перспектива



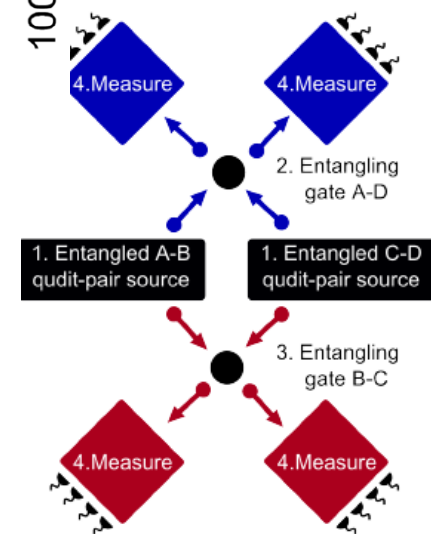
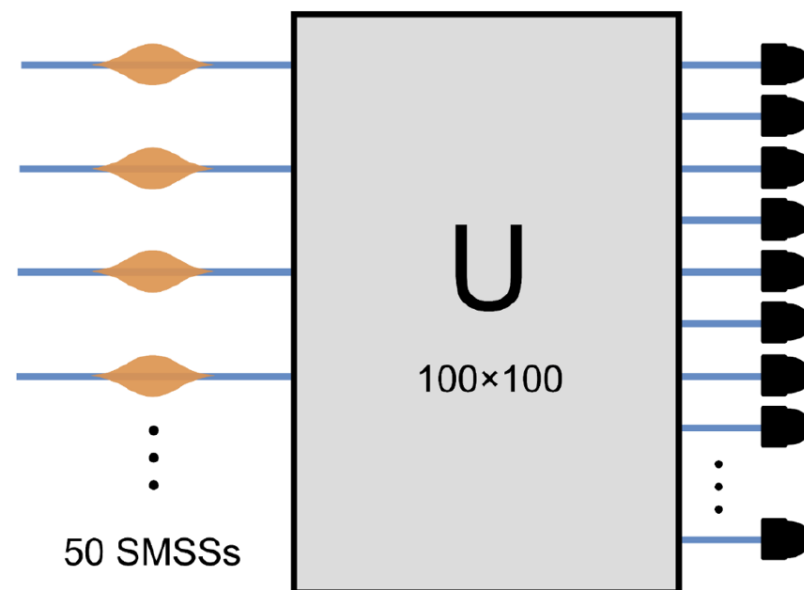
Долгосрочная перспектива:  
баллистическая архитектура

В)



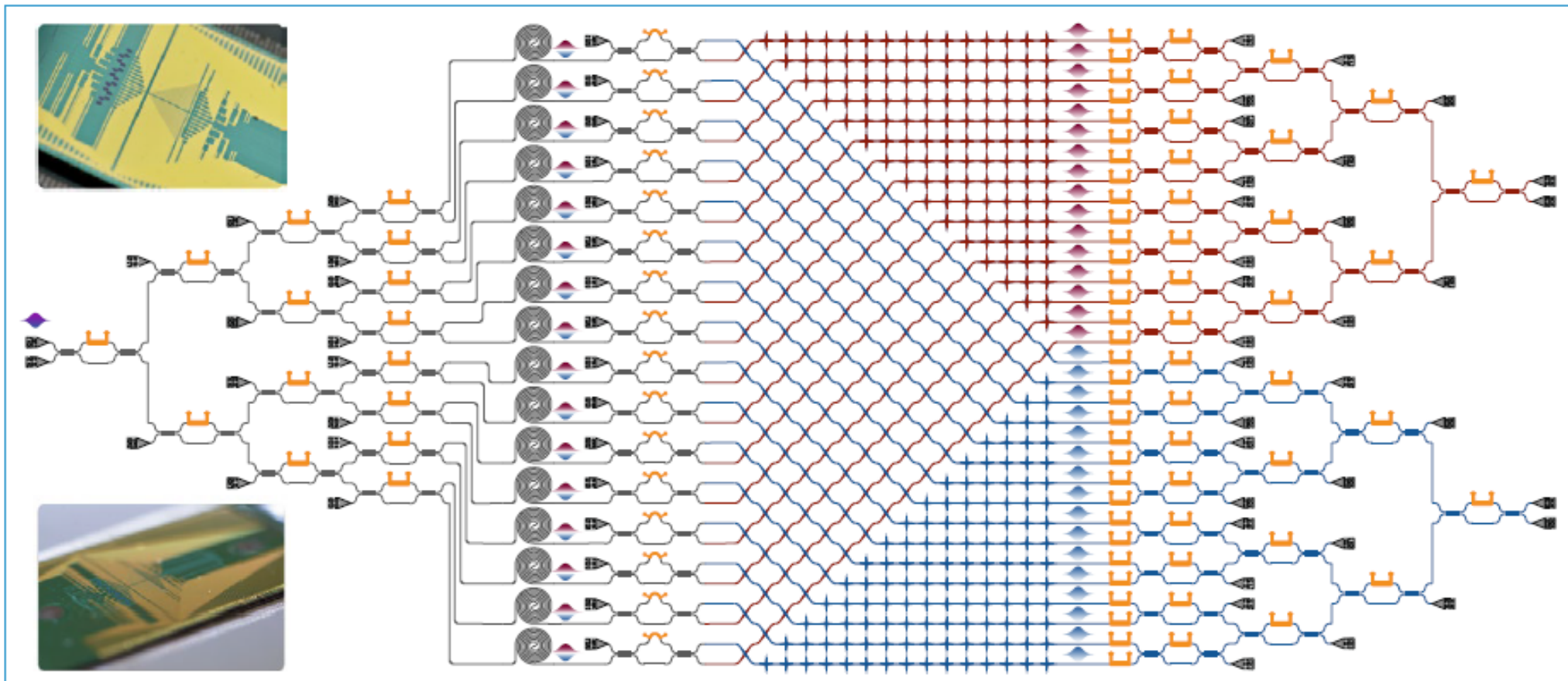
# Ситуация в мире: эксперимент

- Экспериментальная демонстрация квантового превосходства в задаче boson sampling [Zhong H.-S. et al. Quantum computational advantage using photons. Science 370, 6523, 1460-1463 (2020)]
- Обработка до 8 логических кубитов на основе одиночных фотонов [Vigliar C. et al. Error protected qubits in a silicon photonic chip. arXiv:2009.08339v1 (2020)]

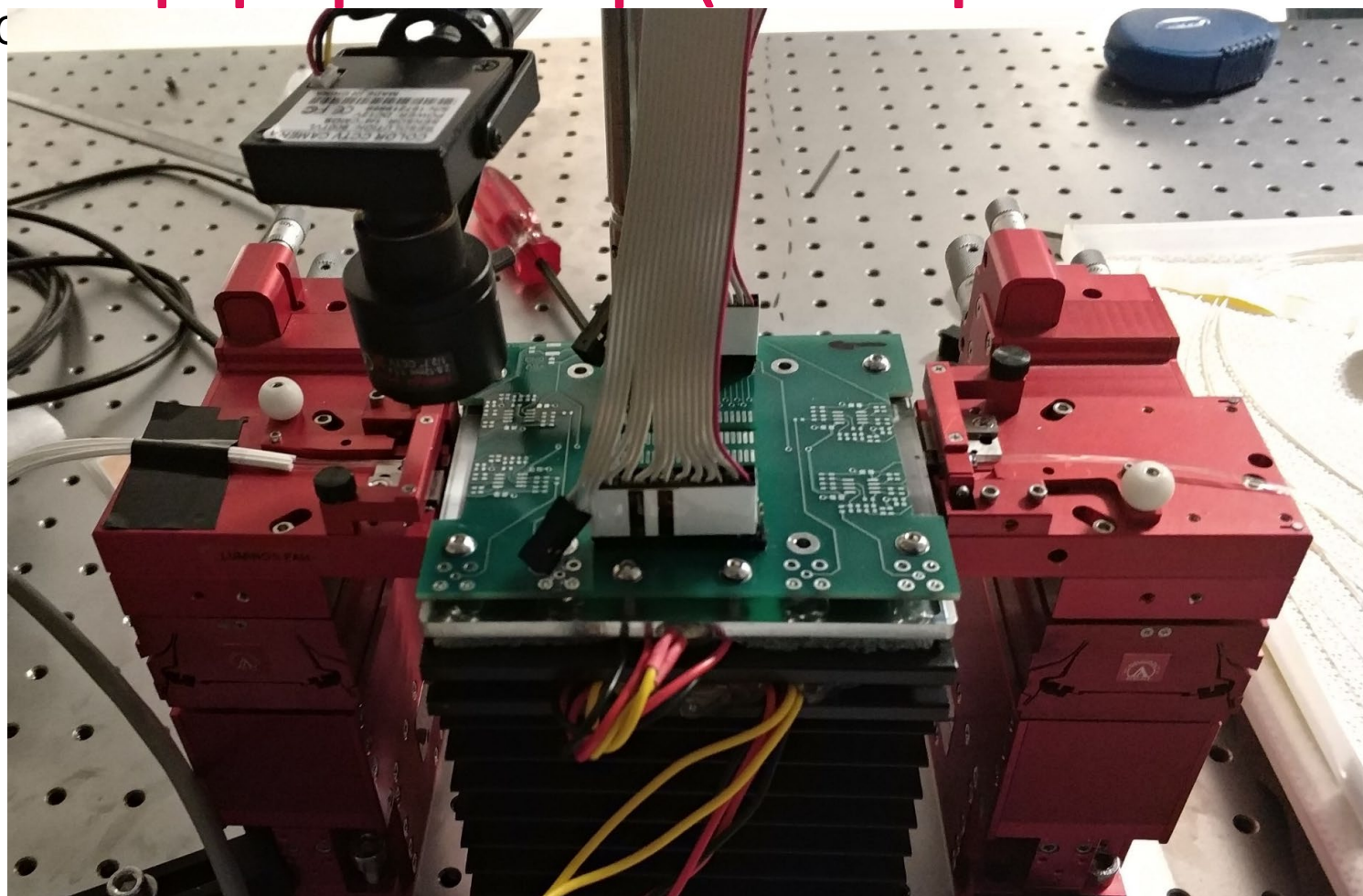




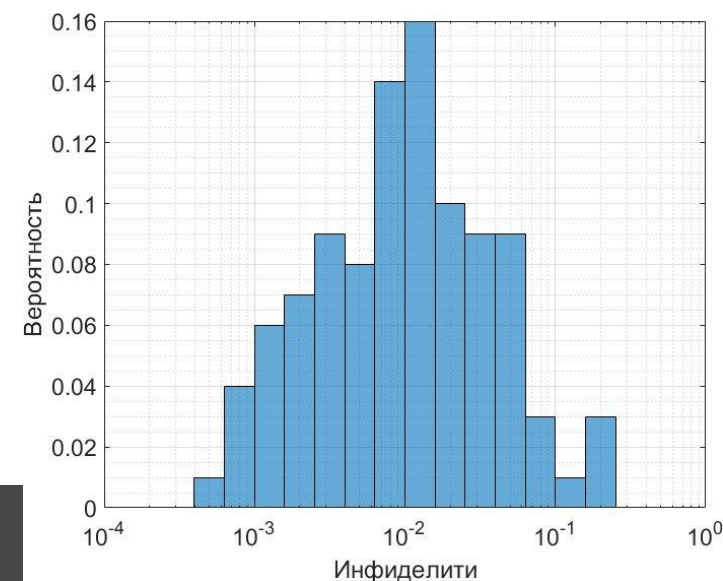
# Пример интегрально-оптической реализации вычислителя



# Восьмиканальный программируемый интерферометр (56 термоэлементов)



Точность реализации  
унитарных преобразований 98%



# Линейно-оптические вычисления: недостатки\*

1. Фотоны – быстрые (“Flying qubits”);
2. Фотоны – дешевые;
3. Низкие значения нелинейных восприимчивостей – фотоны плохо взаимодействуют с окружением
4. Аппаратная и технологическая часть хорошо развита – технология телекоммуникаций, интегральная оптика;
5. Естественная платформа для некоторых квантовых алгоритмов (Quantum Walks, Boson Sampling);
- 6. Вероятностная модель: при учете потерь и ограниченных эффективностей генерации/детектирования компенсируются преимущества масштабирования.**

# КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: ВЫВОДЫ

- Число кубитов и качество логических операций в квантовых вычислителях стабильно растёт;
- Квантовое вычислительное превосходство уже продемонстрировано;
- Есть основания полагать, что даже небольшие NISQ устройства могут дать преимущество в практически важных задачах;
- Квантовые алгоритмы в целом и в приложении оптимизационным задачам в частности – активно развивающаяся область;
- **Речь идет о создании в ближайшие 5 лет среднemasштабных вычислителей, способных продемонстрировать «квантовое преимущество» перед классическими суперкомпьютерами в ряде задач (оптимистичный сценарий).**

# Контактная информация

Электронная почта:

Sergei.kulik@physics.msu.ru

Телефон:

+7 910 484-06-22

Facebook:

----

Сайт:

<https://quantum.msu.ru/ru>



СПАСИБО ЗА ВНИМАНИЕ