Квантовые вычисления: прогнозы и препятствия*

С.П.Кулик

Представлен краткий обзор состояния дел в области квантовых вычислений и обсуждены основные проблемы на пути построения полномасштабных квантовых компьютеров, а также пути их решения.

Ключевые слова: *кубиты, масштабирование, квантовые ошибки, квантовые алгоритмы.*

1. Введение

Квантовые технологии – бурно развивающаяся интердисциплинарная область науки и техники, относящаяся к так называемым сквозным технологиям[1]. Согласно установившейся классификации квантовые технологии включают в себя три больших раздела: квантовые вычисления, квантовые коммуникации и квантовые сенсоры. Уровни технологической готовности трех субтехнологий существенно различаются. Если квантовые вычисления в основном находятся в состоянии фундаментально ориентированных исследований, то в области квантовых коммуникаций и сенсоров успехи выражаются наличием коммерчески доступных устройств, таких как системы квантовой криптографии и/или прецизионные квантовые магнитометры, гравиметры и пр., доведенные, как минимум, до пилотных проектов, демонстрирующих возможности технологии. Другое дело, что эти возможности пока не используются в полной мере. Это связано и с отсутствием рынка, и с консервативностью некоторых отраслей, где имеющиеся решения вполне отвечают обозначившимся вызовам, и с недостатком образования, и с доминированием идеи о том, что квантовые технологии – это технологии отдаленного будущего. Наметившиеся в последние несколько лет положительные тенденции в понимании необходимости развивать эти новые технологии уже сейчас, к тому же подкрепленные солидным финансированием (и в мире, и в РФ, где запущены дорожные карты по квантовым вычислениям и квантовым коммуникациям), являются хорошими предпосылками для психологического и технологического перелома в развитии этой отрасли.

Несмотря на различные цели и задачи, которые ставятся перед тремя субтехнологиями, их фундаментальные физические основы являются общими и сводятся к проблеме исследования того, как законы квантовой физики могут способствовать улучшению технологий приема, передачи и обработки информации. Следует подчеркнуть, что существенным отличием настоящего этапа в развитии квантовых технологий является появившаяся на рубеже 20-го–21-го вв. возможность манипулирования состояниями отдельных квантовых объектов – фотонов, атомов, ионов, молекул. Законы квантовой механики, открытые в 20-м в., прекрасно зарекомендовали себя при описании не только коллективных свойств таких объектов; они дают инструмент для построения уникальных устройств, основанных на универсальной схеме: приготовление квантового состояния – его эволюция – измерение. Эти законы строятся на таких понятиях, как квантовые состояния, суперпозиция, перепутывание, измерение и др., интерпретации которых зачастую противоречат установившимся классическим представлениям о строении поля и вещества, а также взаимодействии между ними. Даже такое понятие, как «суперпозиция», несмотря на то что оно хорошо известно в классической физике – тех ее разделах, которые связаны с волновыми эффектами (оптика, акустика, электродинамика), в квантовой механике сталкивается с некоторыми проблемами при описании известных эффектов.

2. Основные понятия и определения: примеры

Суперпозиция. Например, понятие квантового бита (кубита[2]), представляемого в виде суперпозиции двух базисных состояний $|0\rangle$ и $|1\rangle$ с амплитудами c_1 и c_2,

*Статья подготовлена на основе материалов, представленных на XLVII Вавиловских чтениях по люминесценции, посвященных 132-летию со дня рождения академика С.И.Вавилова (12 апреля 2023 г., ФИАН им. П.Н.Лебедева РАН). Поскольку работа фактически представляет собой доклад, то ее жанр не отвечает канонической научной статье; скорее это «мысли вслух», положенные на бумагу и сопровождаемые некоторыми аргументами.

[1] Сквозные технологии – это передовые научно-технические отрасли, создающие высокотехнологичные продукты и сервисы и оказывающие значительное влияние на развитие экономики и появление новых рынков; к сквозным относятся те технологии, которые одновременно охватывают несколько трендов или отраслей.

С.П.Кулик. Московский государственный университет им. М.В. Ломоносова, физический факультет, Центр квантовых технологий, Россия, 119991 Москва, Ленинские горы, 1, стр. 35; Южно-Уральский государственный университет, лаборатория «Квантовая инженерия света», Россия, 454080 Челябинск, просп. Ленина, 76; e-mail: sergei.kulik@gmail.com

Поступил в редакцию 18 октября 2023 г.

[2] Куби́т (q-бит, от англ. Quantum BIT – квантовый бит), минимальная единица передаваемой или хранимой квантовой информации, аналогичная биту в классической информации (Большая российская энциклопедия).

$$|\Psi\rangle = c_1|0\rangle + c_2|1\rangle, \quad (1)$$

часто интерпретируется как «одновременное существование» квантового объекта в двух состояниях. Действительно, проекционные измерения, выполняемые над состоянием (1), в базисе $|0\rangle$, $|1\rangle$ будут давать исходы, вероятности которых определяются как $P_{1,2} = |c_{1,2}|^2$. Вместе с тем элементарное преобразование поворота SU (2) с эффективными коэффициентами пропускания и отражения t и r,

$$\hat{D} = \begin{pmatrix} t & r \\ -r^* & t^* \end{pmatrix}, \; t = \cos\delta + i\sin\delta\cos(2\chi), \; r = i\sin\delta\sin(2\chi), \quad (2)$$

хорошо известное, например, в поляризационной оптике, переводит состояние (1) в собственное состояние нового базиса, в котором измерения могут давать единственный исход и квантовые флуктуации отсутствуют. Наиболее простым примером такого преобразования служит оператор Адамара

$$H \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (3)$$

обращающий базисные векторы $|0\rangle$, $|1\rangle$ в суперпозиции

$$|D\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |A\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (4)$$

Соответственно, обратное к (3) преобразование переводит суперпозиции (4) в $|0\rangle$, $|1\rangle$. Ни в коей мере не подвергая критике вероятностную интерпретацию суперпозиционных (чистых) состояний в квантовой механике, обращаем внимание на ее другую сторону. Векторы-состояния можно раскладывать в разных базисах в зависимости от удобства и контекста задач; соответственно, исходы измерения в разных базисах могут проявлять вероятностные или детерминированные свойства чистых состояний.

Перепутывание. Другой пример – интерпретация так называемых перепутанных состояний – вообще трудно поддается классическим аналогиям. Действительно, простейшее чистое перепутанное состояние двухкомпонентной (двухкубитной) «1, 2» квантовой системы,

$$|\Psi^-_{1,2}\rangle = \frac{1}{\sqrt{2}}[|0_1\rangle|1_2\rangle - |1_1\rangle|0_2\rangle],$$

имеет нулевую энтропию, в то время как состояния подсистем «1» и «2» являются полностью смешанными и, соответственно, обладают максимальной энтропией. Аналога в классической физике нет: если мы знаем все о составной системе, то нам известно и про состояния образующих ее подсистем!

Измерения. Наконец, последний пример относится к квантовой теории измерений и к постулату Бора: измерение квантовой системы приводит к классическим вероятностным исходам; если над квантовой системой, находящейся в состоянии $|\psi\rangle$, производится измерение, которое описывается оператором M_m, то вероятности исходов различных измерений определяются по правилу $P_m = \langle\psi|E_m|\psi\rangle$, где введены положительно определенные операторы[3] $E_m = M_m^\dagger M_m$, $\sum_m E_m = I$.

[3] Эти операторы известны в квантовой механике как POVM (Positive Operator-Valued Measure) – элементы, связанные с измерениями.

Эти примеры приведены не случайно: далее, опираясь на них, мы проанализируем основные понятия, современное состояние, проблемы и вехи развития субтехнологии «квантовые вычисления». В последнее время наблюдается повышенный интерес к этой отрасли, к сожалению, зачастую «подогретый» не всегда адекватным освещением новостей этой отрасли в масс-медиа. Немаловажную роль играет и созданный ореол загадочности и таинственности квантового мира, понимание закономерностей которого отсутствует не только у граждан, читающих новости, но и у некоторых представителей научного мира, позволяющих себе комментировать то, что они не до конца понимают.

Среди большого числа определений квантового компьютера, встречающихся в литературе, остановимся на таком[4]: это физическое устройство, выполняющее логические операции над квантовыми состояниями путем унитарных преобразований (т. е. сохраняющих энергию), не нарушающих квантовые суперпозиции в процессе вычислений. Для построения полномасштабного квантового компьютера необходимо выполнить несколько критериев, известных как критерии Ди Винченцо [1]:

– масштабируемость;

– надежная инициализация;

– большие времена декогеренции (релаксации) по сравнению с временем срабатывания отдельных гейтов (квантовых логических операций);

– возможность проведения преобразований (манипуляций) над кубитами;

– возможность передачи и считывания состояний кубитов.

С экспериментальной точки зрения устройство, претендующее на выполнение квантовых вычислений, должно:

– обладать хорошо физически определенным квантовым битом информации – кубитом;

– быть в состоянии генерировать полный набор универсальных квантовых гейтов;

– обладать свойством масштабируемости.

3. Масштабирование: ошибки

Свойство масштабируемости в перечне критериев Ди Винченцо в технике и информатике обычно интерпретируется как способность системы справляться с увеличением рабочей нагрузки при добавлении аппаратных ресурсов или как способности системы увеличивать или уменьшать производительность и стоимость при изменении требований к обработке приложений. В приложении к квантовым вычислительным системам масштабируемость – это способность увеличивать число кубитов до уровня, необходимого для решения более крупных и сложных задач.

Свойство масштабируемости – одно из самых тяжелых на пути реализации квантовых вычислителей. Построение квантовых вычислительных схем, решающих осмысленные задачи, требует большого числа кубитов. Вместе с тем увеличению числа задействованных кубитов препятствует несколько процессов, прежде всего релакса-

[4] В качестве альтернативы приведем другое определение, которое, на наш взгляд, в меньшей степени отражает существенные признаки квантового компьютера: это физический компьютер, работа которого основана на уникальных свойствах квантовой физики и принципиально отличается практически от всех существующих компьютеров (которые в совокупности называются классическими).

ция. Кроме того, для выполнения двухкубитных операций требуется их попарное взаимодействие, что далеко не всегда реализуемо с физической и с технической точек зрения. Здесь мы подходим к важному моменту, связанному с балансом между числом кубитов и качеством логических операций, выполняемых над ними. Очевидно, что в физическом мире трудно приготовить начальное состояние системы в заданном виде, трудно добиться идеальных (безошибочных) преобразований и трудно правильно провести измерения финального состояния. Более того, с каждой операцией количество ошибок увеличивается, а надежность снижается!

На рис.1 показаны уровни ошибок одно- и двухкубитных гейтов, а также ошибки, возникающие при обработке/выводе данных для 15 известных вычислительных устройств на основе сверхпроводниковой, ионной и атомной платформ. Видно, что при числе кубитов порядка 10 основной источник ошибок представляют именно двухкубитные операции, а также процедура считывания результата (ссылки на источники указаны ниже в табл.1). Важно отметить, что эти данные получены для так называемых квантовых компьютеров NISQ (Noisy Intermediate-Scale Quantum) – т.е. для среднемасштабных (порядка нескольких десятков кубитов) устройств, в которых не выполняются операции по исправлению ошибок. Другими словами, такие устройства оперируют с физическими кубитами, подверженными и декогеренции, и «шумным» гейтам.

На рис.2 показан предельный уровень ошибок для выполнения полномасштабных квантовых вычислений в логарифмическом масштабе – то, что имеется сейчас, в эпоху NISQ, и что ожидается в ближайшем будущем [2]. Выход за рамки концепции NISQ предполагает использование кодов коррекции ошибок и переход к помехоустойчивым квантовым вычислениям. В правой части приведенной шкалы отложены уровни ошибок для так называемых транзисторов ENIAC (Electronic Numerical Integrator and Computer), использованных в электронных цифровых вычислителях общего назначения, которые можно перепрограммировать для решения широкого спектра задач. Видно, что необходимый уровень ошибок выходит далеко за пределы достигнутой сегодня точности.

Обратим внимание на следующее обстоятельство. Когда в научной статье сообщается об уровне ошибок (одно- или двухкубитных гейтов), зачастую трудно понять, если об этом не говорится непосредственно, для какой выборки кубитов приводятся эти значения: для каж-

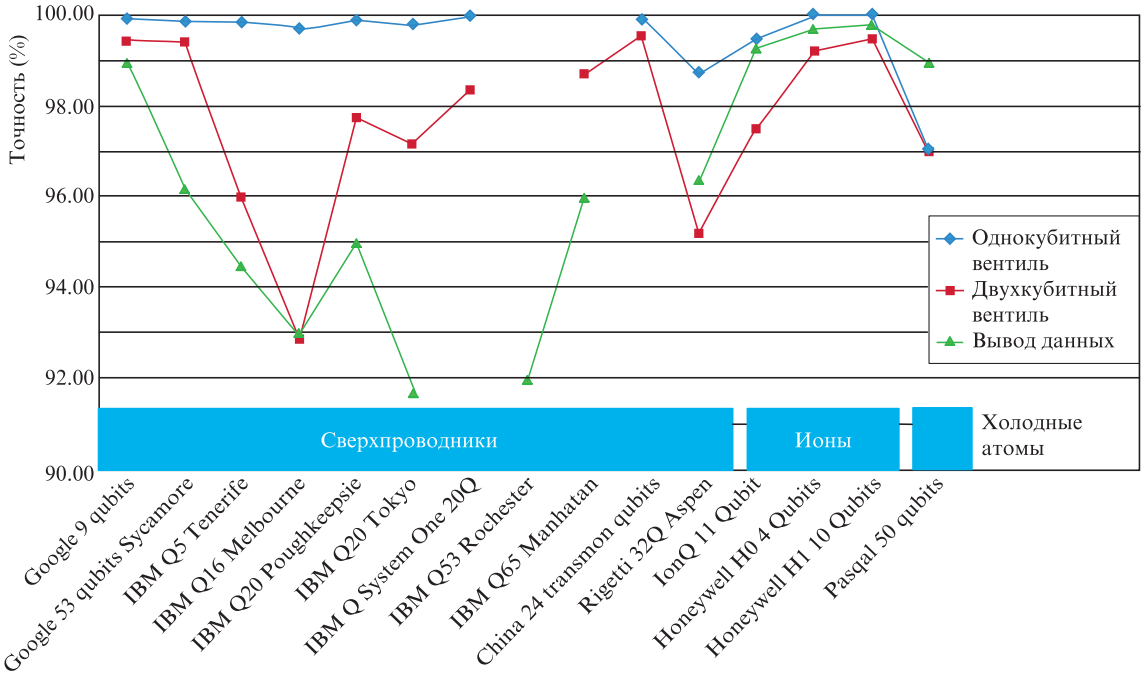

Рис.1. Точность выполнения одно- и двухкубитных операций, а также операции считывания результата для трех физических платформ квантовых вычислений.

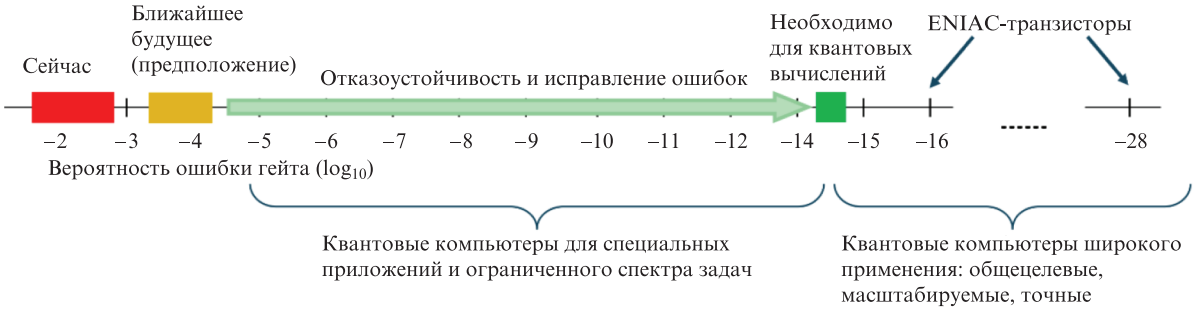

Рис.2. Предельный уровень ошибок для выполнения полномасштабных квантовых вычислений.

Табл.1. Сравнение разных физических платформ – кандидатов на построение квантового компьютера.

Платформа	Масштабируемость (число кубитов в регистре)	Время когерентности (с)	Время срабатывния гейта (1 кубит/ 2 кубита) (мкс)	Фиделити (1 кубит/2 кубита)	R-фактор (1 кубит/ 2 кубита) $\times 10^6$	Источник
Ионы	218	5500	5/25	0.99998/0.999	1100/220	[4, 5]
Нейтральные атомы	256	3	2/04	0.999/0.995	1.5/7.5	[6, 7]
Сверхпроводники	433	0.5	0.02/0.03	0.9998/0.9987	25/16.7	[8–10]
Фотоны	более 1000	∞	менее 0.001/0.01	более 0.9999/0.994	∞	[11–13]
Центры в алмазах	10	60	0.01/0.7	0.99995/0.992	6000/85.7	[14, 15]
Примеси /КТ в кремнии	2 [кубита($2e^-$)] 3 [кубита(2ядра +$1e^-$)] /6	30 [спин ядра] 0.5 [спин e^-] /0.028	0.0008/0.025	99.99/99.96	1.12/0.28	[16–19]

дого кубита (или пары кубитов), для выбранного набора, имеются ввиду лучшие значения или среднее по ансамблю. Это обстоятельство является решающим для оценки адекватности ресурсного обеспечения работы конкретного устройства. В этой связи представленные на рис.1 значения ошибок надо воспринимать критически: очевидно, что если они относятся к лучшим из измеренных, то оценки могут радикально поменяться в сторону уменьшения для усредненных значений!

В табл.1 представлены некоторые параметры квантовых вычислительных устройств, реализованных на основных физических платформах. Эти данные позволяют в некоторой степени оценить ситуацию с NISQ-устройствами, сравнить их между собой и, возможно, сделать выводы о перспективах той или иной платформы [3]. Отметим, что приведенные данные взяты из открытых источников и к ним следует относиться осторожно; во всяком случае следует учитывать аргументы, изложенные выше.

Рассматривались следующие физические платформы: ионы в линейных ловушках, нейтральные атомы в микродипольных ловушках, сверхпроводящие цепи, фотонные чипы (эта платформа реализована на вероятностных гейтах), центры окраски в алмазах, а также примеси и квантовые точки (КТ) в кремнии. В качестве параметров выбраны: число кубитов в регистре, время когерентности, времена срабатывания и фиделити (fidelity) одно- и двухкубитных гейтов; кроме того, приведены значения так называемого R-фактора, равного отношению времени когерентности к времени срабатывания гейта. Отметим, что лучшие результаты для каждой платформы были получены в разных экспериментах, ссылки на которые даны в табл.1. Подробный анализ недостатков и преимуществ той или иной платформы выходит за рамки настоящей работы, однако отметим, что вряд ли какая-то платформа является однозначным лидером среди кандидатов на построение квантового компьютера; в каждой из платформ есть недостатки и преимущества.

4. Масштабирование: метрики

Что касается кодов коррекции ошибок, то их разбор выходит далеко за пределы данной работы, но их краткая сводка – по результатам [20] – представлена на рис.3. Как правило, для устойчивой работы кодов требуется большое количество логических кубитов, которые можно использовать и для оптимизации исправления ошибок, например, с помощью поверхностных и цветовых кодов. Сегодня ни один из известных квантовых компьютеров не обладает достаточными ресурсами ни для операций с логическими кубитами, ни для задействования кодов коррекции ошибок. Более того, число необходимых физических кубитов на один логический кубит сравнимо или превышает число физических кубитов, доступных в настоящее время. Поэтому проблема масштабирования является одной из наиболее острых; она упирается и в качество, и в количество доступных ресурсов. Действительно, если квантовый процессор оперирует с n кубитами, то вне зависимости от того, хорошо или плохо он работает, процессору доступно не более чем 2^n состояний. С другой стороны, если процессор плохо контролируется и/или сильно шумит, то некоторые из этих n кубитов могут оказаться лишними, т. е. полное пространство состояний 2^n будет недоступно. В этой связи и возникает обсуждавшийся выше вопрос: чему равно доступное пространство состояний для квантового процессора?

Для преодоления неоднозначности, связанной с адекватной интерпретацией необходимых для квантовых вычислений ресурсов, было сделано несколько попыток ввести единые метрики. Квантовый объем (V_Q) – это метрика, предложенная компанией IBM, выражаемая одним числом и предназначенная для инкапсуляции производительности квантовых компьютеров. Случайные состояния могут генерироваться случайными программами (схемами), но число необходимых шагов (глубина схемы) растет с увеличением количества кубитов. Таким образом, утверждение о том, что квантовый объем процессора составляет не менее 2^n, эквивалентно тому, что возможно надежно запускать случайную квантовую схему с шириной и глубиной, равными как минимум n.

Объем V_Q [21] учитывает число кубитов, уровень ошибок и связность кубитов (т. е. какие пары кубитов могут быть запутаны):

$$\log_2 V_Q = \mathrm{argmax}_m[\min(m, d(m))], \quad (5)$$

где $m < n$ – число кубитов, а $d(m)$ – максимальная глубина случайных m-кубитных цепочек, по результатам запуска которых доля «тяжелых» выходов с достоверностью превышает 67% (под «тяжелыми» выходами понимаются битовые строки, вероятность наблюдения которых при идеальном выполнении данной цепочки выше медианного значения). Протокол по вычислению квантового объема проверяет, насколько хорошо квантовый компьютер может запускать схему, состоящую из случайного набора двухкубитовых гейтов, действующих параллельно на

Рис.3. Основные коды квантовой коррекции ошибок согласно [20] (CTQEC – Continuous-time quantum error correction).

подмножестве кубитов данного устройства. У этих схем есть ширина, означающая число задействованных кубитов, и глубина, означающая количество дискретных временных шагов, в течение которых схема может запускать гейты до того, как кубиты подвергнутся декогерентизации. Протокол позволяет квантовому компьютеру переписывать исходную схему в такую, которую он действительно может запустить, в зависимости от числа доступных гейтов и того, как кубиты связаны между собой. Таким образом квантовый объем определяет самую большую квадратную схему (где ширина и глубина равны), способную работать на данном квантовом устройстве[5]. Конкретный пример: предположим, что у нас есть устройство с 20 кубитами, и оказывается, что мы надежно получаем выходные данные для схем глубиной до 4 на любом наборе из четырех кубитов. Тогда $\log_2 V_Q = 4$.

Однако предложенная IBM-метрика, применяемая к сверхпроводниковой платформе квантовых вычислений, оказывается не вполне корректной для тех платформ, в которых точность выполнения операций значительно выше, например для ионной. Компания IonQ предложила в качестве метрики так называемые алгоритмические кубиты (AQ), которые определяются как наибольшее количество идеальных кубитов, которые можно использовать для типичной квантовой программы/схемы. Если не использовать коды коррекции, то метрики находятся в простом соотношении: $\mathrm{AQ} = \log_2 V_Q$. Более консервативное утверждение состоит в замене равенства на неравенство, $\mathrm{AQ} \geqslant \log_2 V_Q$, поскольку в случае характеризации V_Q требуется проведение произвольной двухкубитной операции, в то время как для AQ достаточно некоторой конкретной двухкубитной операции.

Часто для характеризации необходимых для квантовых вычисления ресурсов используется понятие «бенчмарк» (benchmark). Под бенчмарком понимается набор квантовых схем (набор тестов) вместе с инструкциями по их запуску (план эксперимента), процедура анализа для обработки результатов и, наконец, правило интерпретации для получения высокоуровневых данных [22].

Бенчмарки часто предназначены для измерения одной или нескольких метрик, например квантового объема. Существует множество разнообразных бенчмарков, применяемых для измерения других конкретных показателей. Рандомизированный бенчмаркинг (Randomized Benchmarking [23]) предназначен для измерения фиделити[6]. Томография набора гейтов с помощью длинных последовательностей (Long-Sequence Gate Set Tomography [24]) – протокол, в котором используется семейство схем для измерения параметров набора гейтов, описывающих зашумленные операции процессора, – определяет набор тестов, который можно легко переформулировать в бенчмарк. Однако бенчмарки не обязательно ассоциируются с четко определенными метриками.

Какие именно внутренние и/или синтетические метрики/показатели/бенчмарки будут отражать те или иные аспекты производительности квантовых компьютеров, в настоящее время совсем не ясно. Квантовый объем представляется хорошей интегральной метрикой, хотя, как показывает пример с алгоритмическими кубитами, и не единственной в бенчмаркинге квантовых компьютеров. При отсутствии четких требований к метрикам и бенчмаркам, судя по всему, потребуется множество таких тестов, которые могут выражаться друг через друга, а могут и не выражаться. Во всяком случае деятельность по выявлению критериальных признаков, позволяющих

[5] Другое определение квантового объема: произведение числа кубитов на число операций, которые возможно осуществить за определенный промежуток времени.

[6] К сожалению, как и во многих других случаях, для fidelity пока не выработан адекватный русскоязычный термин.

	«Эра» NISQ 3-5 лет	Всеобщее квантовое превосходство Более 10 лет	Полномасштабный помехоустойчивый квантовый компьютер Более 20 лет
Технические достижения	Устранение ошибок	Исправление ошибок	Модульная архитектура
Пример влияния на бизнес	Симуляторы задач материаловедения	Оценки финансовых рисков в близком к реальному времени (например, для инвестиционных фондов)	Дизайн лекарств, содержащих большие биопрепараты, с минимальными побочными эффектами
Операционная прибыль	2-5 млрд. долларов	25-50 млрд. долларов	450-850 млрд. долларов

Рис.4. Фазы зрелости квантовых вычислительных систем.

сравнивать производительность и другие показатели работы квантовых вычислительных устройств, в настоящее время активно развивается и ее значение трудно недооценить.

Подводя итог этой части, отметим, что эпоха универсального квантового компьютера находится сильно в правой части временной шкалы: практическое использование кодов коррекции ограничено как низким качеством приготовления начального состояния кубитов в квантовом регистре[7], так и применяемыми к ним гейтами. Доступной альтернативой является парадигма NISQ – шумящие квантовые компьютеры с небольшим (до 100) числом кубитов. Именно на таких машинах уже реализованы некоторые квантовые алгоритмы – продемонстрирован квантовый отжиг, сортировка бозонов и реализованы первые квантовые симуляторы. Отметим, что здесь и ниже речь не идет о так называемых квантовых эмуляторах[8], предназначенных для решения задач при помощи квантовых алгоритмов на классических компьютерах. Мы рассматриваем именно квантовые вычислительные устройства – универсальные, аналоговые (симуляторы), на основе непрерывных или дискретных переменных, топологические, компьютеры на основе измерений (Measurement based), на основе квантового отжига и др.

5. Перспективы

Интересна оценка перспектив использования квантовых компьютеров в решении практически полезных задач. По данным консалтингового агентства Boston Consulting Group (рис.4) в ближне-, средне- и долгосрочных перспективах, которые соответственно разграничиваются интервалами до пяти, свыше десяти и свыше двадцати лет, на физическом уровне работа с квантовыми вычислительными устройствами будет сконцентрирована на устранении ошибок (эпоха NISQ), их исправлении и построении квантовых компьютеров с модульной архитектурой. По типам решаемых задач эти интервалы будут характеризоваться построением симуляторов (5 лет), использованием, например, в банковской сфере (свыше 10 лет) в ряде оптимизационных задачах и, наконец, в перспективе до 30 лет переходом к решению задач материаловедения – на уровне, превосходящем современные классические суперкомпьютеры (рис.5).

Перечень задач, эффективно решаемых на квантовых компьютерах, хорошо известен; он сводится к задачам комбинаторной оптимизации, решению систем линейных алгебраических (СЛАУ) и дифференциальных уравнений, задач факторизации и др. Наверное, следует осторожно относиться к оценкам реализации этих и других квантовых алгоритмов: во-первых, потому, что таких оценок уже было множество и каждый раз сроки сдвигались вправо, а во-вторых, прогнозирование физических результатов – вообще дело неблагодарное, и масштабирование с параллельным улучшением точности операций пока сталкивается с серьезными трудностями.

На рис.6 собраны данные из различных литературных источников по фактическому состоянию и прогнозированию создания квантовых вычислительных устройств на разных платформах. Обращаем внимание на обещанную компанией IONQ демонстрацию полномасштабного квантового превосходства в текущем 2023 г., правда, непонятно для какого алгоритма.

Как уже упоминалось выше, указания числа кубитов без упоминания о точности одно- и двухкубитных операций особого смысла не имеют; именно поэтому были введены более адекватные меры ресурсных возможностей квантовых вычислителей, такие как квантовый объем и алгоритмические кубиты (см. разд.4).

6. Оценки квантовых ресурсов для некоторых задач криптоанализа

Рассмотрим несколько примеров оценки необходимых ресурсов для задач криптоанализа – числа логических кубитов, элементарных квантовых вентилей – при

[7] Квантовый регистр – физическая система, позволяющая выполнять инициализацию, хранение, преобразование и считывание квантовой информации.

[8] Отнюдь не умаляя роли квантовых эмуляторов, заметим, что они выполняют лишь методическую задачу адаптации квантовых алгоритмов к простым, в основном оптимизационным задачам, а также «обкатки» соответствующего программного обеспечения.

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)	• Оптимизация сети (например, для авиалиний, такси) • Оптимизация цепочек поставок и/или логистики • Оптимизация финансовых сервисов
Решение систем диф. уравнений	Моделирование поведения сложных систем, (например, уравнение Навье-Стокса в гидродинамике)	• Моделирование гидродинамики для дизайна - автомобильной и авиационной техники; • Моделирование медицинских приложений (например, анализ кровотока); • Молекулярное моделирование новых материалов и/или лекарств
Решение систем линейных уравнений	Задачи машинного обучения с использованием матрицы диагонализации (например в задаче кластеризации)	• Управление рисками в финансовой сфере • Классификация последовательностей ДНК • Маркетинг и сегментация клиентов
Задача факторизации	Криптография и компьютерная безопасность, (например, RSA)	• Дешифрование и/или взлом кода

Рис.5. Перспективные задачи для квантовых вычислений.

№	компания	Тип кубита	Срок создания Кв. компьютера
1	IBM	сверхпроводники	Сегодня: 137 кубитов Начало 2022: 433 кубитов “Osprey”; Конец 2023 - 1121 кубитов “Condor”
3	Google	сверхпроводники	Квантовый компьютер с кодами коррекции ошибок, способный выполнять полезные вычисления, будет построен к 2029г.
4	IONQ	ионы	Прогнозируемый квантовый объем - 4 млн. 2023 год – демонстрация полномасштабного квантового превосходства. 2028 год – 1024 алгоритмических кубита
4	Honeywell	ионы	2021г. -квантовый объем 1024.
5	PsiQuantum	фотоны	2025г. - 1 млн. кубитов, 1000 логических кубитов
6	Xanadu	фотоны	1 млн. кубитов с исправлением ошибок (срок не указан)
7	Pascal	Нейтральные атомы (Rb)	1000 физических кубитов (без сроков)
8	QuERA	Нейтральные атомы	2021 г.- 256-512 физических кубитов; 2022 г. - полностью программируемый КвК с 64 кубитами (симулятор) 2024 – полностью программируемый КвК с 1024 кубитами.
9	D-Wave	Гибридная платформа: квантовый отжиг и сверхпроводниковые кубиты	2023-2024гг – 7000 кубитов

Рис.6. Прогнозируемые сроки создания квантовых вычислительных устройств от лидирующих компаний (крестиками выделены реализованные к сегодняшнему дню параметры).

переборном поиске ключа шифрования для алгоритма шифрования AES [25] с разной длиной ключа [26]. Как правило, именно такие задачи взлома асимметричных классических протоколов являются показательными как для обоснования угроз квантового компьютера по дешифрованию, так и для необходимости развития постквантовых алгоритмов и квантовой криптографии.

В табл.2 показаны оценки необходимого числа логических кубитов в случае использования идеальных (нешумящих) квантовых гейтов в алгоритме Гровера. Задейст-

Табл.2. Оценки необходимых ресурсов при полном переборном поиске ключа шифрования алгоритмом Гровера для алгоритма шифрования AES с длиной ключа 128, 192 и 256 бит.

Длина ключа k (бит)	Гейты		Глубина схемы	Число логических кубитов
	T	Клиффорд		
128	1.19×2^{86}	1.55×2^{86}	1.16×2^{81}	2953
192	1.81×2^{118}	1.17×2^{119}	1.32×2^{113}	4449
256	1.41×2^{151}	1.83×2^{151}	1.57×2^{145}	6681

вованы гейты двух типов – из семейства Клиффорда (операторы Адамара, фазового сдвига π/2, управляемого NOT и операторы Паули):

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\quad S=\begin{pmatrix}1 & 0\\ 0 & \exp(\mathrm{i}\pi/2)\end{pmatrix},\quad CNOT=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix},$$

(6)

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad Y=\begin{pmatrix}0 & -\mathrm{i}\\ 1 & 0\end{pmatrix},\quad Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

и так называемые *T*-гейты:

$$T=\begin{pmatrix}1 & 0\\ 0 & \exp(\mathrm{i}\pi/4)\end{pmatrix}. \qquad (7)$$

Обращаем внимание на оценку числа логических кубитов: даже для короткого 128-битного ключа это число составляет почти три тысячи. Видно, что из-за большой глубины схемы развертывания всей итерации Гровера представляется крайне сложным реализовать данный алгоритм на реальном физическом квантовом компьютере даже при использовании идеальных вентилей (т.е. без коррекции ошибок)!

В табл.3 приведены данные анализа для оптимизированных квантовых алгоритмов полного перебора ключей для алгоритма шифрования AES (и криптографических хэш-функций) с разной длиной ключа при различных величинах вероятности ошибки на вентиль [27]. Оценки проводились разными методами в цикле работ группы M.Mosca в 2020–21 гг.; рассматривались так называемые отказоустойчивые (fault-tolerant) реализации квантового компьютера при использовании поверхностных кодов коррекции ошибок [28] как наиболее перспективного кандидата на отказоустойчивость.

Обратим внимание на приведенные в табл.3 значения числа логических кубитов, которые даже при короткой длине ключа 128 бит оказываются порядка 10000. Взлом же 2048-битного ключа шифрования AES потребует около 18 тыс. логических или порядка 18 млн физических кубитов.

Отметим, что для указанных в табл.3 данных уязвимых криптографических схем с симметричным ключом AES квантовые ресурсы представлялись в виде специфической метрики (см. разд.4) – однозначного числа, которое примерно представляет собой произведение размерности пространства (общее число физических кубитов), занимаемого квантовой схемой, на время, необходимое для ее запуска (время пропорционально его глубине, т.е. числу непараллельных операций). Эта метрика допускает компромисс между пространством и временем: в широком диапазоне соответствующих параметров можно сократить время, необходимое для запуска квантовой схемы, увеличив число кубитов (распараллеливание) и, наоборот, сохраняя при этом произведение между пространством и временем (почти) постоянным. В этом случае квантовые ресурсы можно рассматривать как «инвариант» реализации алгоритма, грубо определяющий эффективность работы квантовой схемы. В принципе, можно свободно выбирать любые пары «время/количество физических кубитов» при сохранении соответствующего квантового ресурса постоянными. В контексте рассмотренных выше метрик здесь квантовые ресурсы представляются в единицах мегакубит-дней, т.е. миллионов кубитов, необходимых для взлома схемы за 24 ч (сутки).

7. Заключение

Значительный прогресс в технике физического эксперимента в конце 20-го – начале 21-го вв. обусловил и бурный рост семейства технологий, ставящих своей целью построение квантовых вычислительных устройств. Необходимые для этого теоретические основы можно считать хорошо разработанными на протяжении последних 30 лет; проблема состоит в том, каким образом реализовать имеющиеся теоретические знания в конкретные устройства так, как это было сделано во второй половине 20-го в. с классическими вычислителями.

В этой работе в основном был сделан акцент лишь на одном критериальном аспекте квантовых вычислений – масштабировании при учете квантовых ошибок. На нескольких примерах показаны масштабы «бедствия» – оценки необходимых ресурсов (табл.2 и 3) вряд ли можно назвать оптимистическими. Вместе с тем автор, давно работающий в области квантовых технологий, отнюдь не является пессимистом; скорее занимаемая им позиция относится к разряду «реалистичных оптимистов».

Однако известно большое число работ, в которых делаются оптимистические оценки. Например, при использовании сопоставимых вычислительных мощностей алгоритм квантового отжига дает лучшее качество реше-

Табл.3. Оценки оптимизированных квантовых алгоритмов полного перебора ключей для алгоритма шифрования AES при различных вероятностях ошибки на гейт для длины ключа 128/192/256 бит.

Алгоритм шифрования	p_g	Оценки 2020 г.			Оценки 2021 г.		
		s_q	n_l	n_p	s_q	n_l	n_p
AES-128	10^{-3}	101.66	15265	7.17×10^8	98.95	10954	4.04×10^9
	10^{-5}	97.19	2545	1.77×10^6	94.2	7564	1.74×10^7
AES-192	10^{-3}	137.39	163793	2.93×10^9	135.29	62156	1.12×10^{10}
	10^{-5}	132.81	23393	7.81×10^6	130.67	11756	6.53×10^7
AES-256	10^{-3}	170.49	218465	6.56×10^9	167.67	63884	1.12×10^{10}
	10^{-5}	166.0	34865	1.61×10^7	163.82	13484	1.15×10^8

Примечание: p_g – вероятность ошибки на гейт; s_q – параметр секретности (или параметр квантовой безопасности), определяемый как логарифм по основанию двойки от числа фундаментальных операций (в данном случае циклов поверхностного кода), необходимых для взлома схемы; n_l – число логических кубитов; n_p – число физических кубитов.

ний задач оптимизации, чем QAOA – квантовый алгоритм приближенной оптимизации для квантового компьютера с гейтовой архитектурой. Среди множества примеров выделим развивающуюся в последнее время тему оптической реализации квантовых алгоритмов методами когерентной машины Изинга [29–31]. Сегодня большое значение уделяется разработке эмуляторов, в том числе основанных на распараллеливании алгоритма приближенного решения масштабных задач QUBO. Они позволят предварительно тестировать те же алгоритмы квантового отжига еще до появления доступа к реальному квантовому компьютеру и реализовывать на практике квантово-вдохновленные алгоритмы.

Подводя итог, отметим, что следующие 10–20 лет обещают быть чрезвычайно интересными: «квантовая гонка» на пути построения квантового вычислительного устройства, способного решать практически важные задачи эффективнее, чем это делает классический суперкомпьютер, находится в самом разгаре. Непонятными остаются ответы на два вопроса: когда Природа позволит Человеку это сделать и сколько ему придется за это заплатить?

Работа выполнена при поддержке Министерства науки и высшего образования РФ на базе ФГАОУ ВО «ЮУрГУ (НИУ)» (соглашение № 075-15-2022-1116), а также в рамках Программы развития МГУ (проект № 23А-Ш06-05).

1. DiVincenzo David P. *Fortschr. Phys*., **48**, 771 (2000).
2. Urbanek M., Nachman B., de Jong W.A. *Phys. Rev. A*, **102**, 022427 (2020).
3. Cheng B., Deng X.-H., Gu X., Yu He, Hu G., Huang P., Li J., Lin B.-C., Lu D., Lu Y., Qiu C., Wang H., Xin T., Yu S., Yung M.-H., Zeng J., Zhang S., Zhong Y., Peng X., Nori F., Yu D. *Front. Phys*., **18** (2), 21308 (2023).
4. Yao R., Lian W.-Q., Wu Y.-K., Wang G.-X., Li B.-W., Mei Q.-X., Qi B.-X., Yao L., Zhou Z.-C., He L., Duan L.-M. *Phys. Rev. A*, **106**, 062617 (2022).
5. Zhang S., Lu Y., Zhang K., Wentao Chen, Li Y., Zhang J.-N., Kim K. *Nat. Commun*., **11**, 587 (2020).
6. Wintersperger K., Dommert F., Ehmer T., Hoursanov A., Klepsch J., Mauerer W., Reuber G., Strohm T., Yin M., Luber S. ArXiv:2304.14360v2 [quant-ph] (2023).
7. Bluvstein D., Levine H., Semeghini G., Wang T.T., Ebad S., Kalinowski M., Keesling A., Maskara N., Pichler H., Greiner M., Vuleti V., Lukin M.D. *Nature*, **604**, 451 (2022).
8. Zhu D., Jaako T., He Q., Rabl P. *Phys. Rev. Appl*., **16**, 014024 (2021).
9. Wang C., Li X., Xu H., Li Z., Wang J., Yang Z., Mi Z., Liang X., Su T., Yang C., Wang G., Wang W., Li Y., Chen M., Li C., Linghu K., Han J., Zhang Y., Feng Y., Song Y., Ma T., Zhang J., Wang R., Zhao P., Liu W., Xue G., Jin Y., Yu H. *NPJ Quantum Inf*., **8**, 3 (2022).
10. https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two.
11. Mower J., Harris N.C., Steinbrecher G.R., Lahini Y., Englund D.R. *Phys. Rev. A*, **92**, 032322 (2015).
12. Uppu R., Midolo L., Zhou X., Carolan J., Lodahl P. *Nat. Nanotechnol*., **16**, 13081317 (2021).
13. Shi S., Xu B., Zhang K., Ye G.-S., Xiang D.-S., Liu Y., Wang J., Su D., Li L. *Nat. Commun*., **13**, 4454 (2022).
14. Pezzagna S., Meijer J. *Appl. Phys. Rev*., **8**, 011308 (2021).
15. Shandilya P.K., Flågan S., Carvalho N.C., Zohari E., Kavatamane V.K., Losby J.E., Barclay P.E. *J. Lightwave Technol*., **40**, 7538 (2022).
16. He Y., Gorman S.K., Keith D., Kranz L., Keizer J.G., Simmons M.Y. *Nature*, **571**, 371 (2019).
17. Mądzik M.T., Asaad S., Youssry A., Joecker B., Rudinger K.M., Nielsen E., Young K.C., Proctor T.J., Baczewski A.D., Laucht A., Schmitt V., Hudson F.E., Itoh K.M., Jakob A.M., Johnson B.C., Jamieson D.N., Dzurak A.S., Ferrie C., Blume-Kohout R., Morello A. *Nature*, **601**, 348 (2022).
18. Muhonen J.T., Dehollain J.P., Laucht A., Hudson F.E., Kalra R., Sekiguchi T., Itoh K.M., Jamieson D.N., McCallum J.C., Dzurak A.S., Morello A. *Nat. Nanotechnol*., **9**, 986 (2014).
19. Muhonen J.T., Laucht A., Simmons S., Dehollai J.P., Kalra R., Hudson F.E., Freer S., Itoh K.M., Jamieson D.N., McCallum J.C., Dzurak A.S., Morello A. *J. Phys. Condens. Matter*, **27**, 154205 (2015).
20. Li J. *IEEE Access*., **8**, 46998 (2020).
21. Cross A.W., Bishop L.S., Sheldon S., Nation P.D., Gambetta J.M. *Phys. Rev. A*, **100**, 032328 (2019).
22. Blume-Kohout R., Young K.C. *Quantum*, **4**, 362 (2020).
23. Emerson J., Alicki R., Zyczkowski K. *J. Opt. B: Quantum Semiclassical Opt*., **7**, 347 (2005).
24. Blume-Kohout R., Gamble J.K., Nielsen E., Rudinger K., Mizrahi J., Fortier K., Maunz P. *Nat. Commun*., **8**, 4485 (2017).
25. NIST. Specification for the Advanced Encryption Standard (AES) (FIPS PUB 197, 2001).
26. Grassl M., Langenberg B., Roetteler M., Steinwandt R., in *Post-Quantum Cryptography* (Springer, 2016, pp 29–43).
27. Gheorghiu V., Mosca M. *GRI Quantum Risk Assessment Reports* (2018–2021); https://globalriskinstitute.org.
28. Fowler A.G., Mariantoni M., Martinis J.M., Cleland A.N. *Phys. Rev. A*, **86**, 032324 (2012).
29. Yamamoto Y., Aihara K., Leleu T., Kawarabayashi K., Kako S., Fejer M., Inoue K., Takesue H. *NPJ Quantum Inf*., **3**, 49 (2017).
30. Böhm F., Verschaffelt G., Van der Sande G. *Nat. Commun*., **10**, 3538 (2019).
31. Cen Q., Ding H., Hao T., Guan S., Qin Z., Lyu J., Li W., Zhu N., Xu K., Dai Y., Li M. *Light Sci. Appl*., **11**, 333 (2022).