Квантовый компьютинг в области ИБ:
мифы, реалии, прогнозы

Андрей РЫБКИН,
старший исследователь, Центр научных исследований и перспективных разработок, компания «ИнфоТеКС»

Алексей МОИСЕЕВСКИЙ,
аспирант, Центр квантовых технологий, МГУ имени М. В. Ломоносова

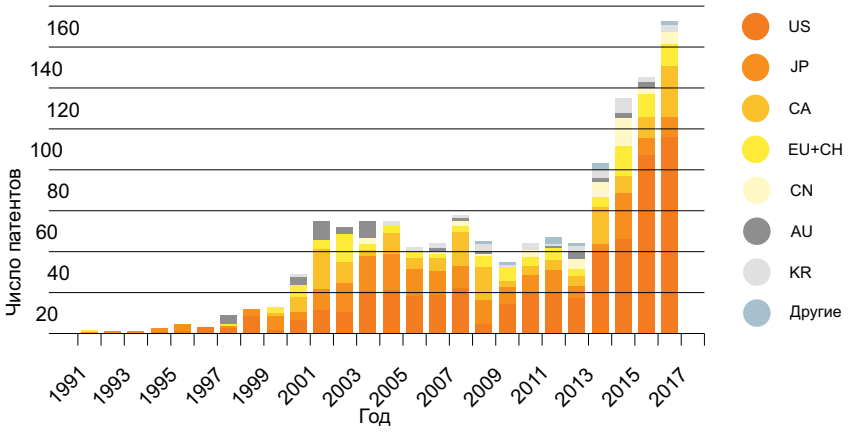
Где находится предел возможностей современного компьютера? Сможет ли достаточно мощный вычислитель с течением времени справиться с любой поставленной задачей или существуют проблемы, которые компьютерам в нашем обычном понимании принципиально неподвластны? Бурное развитие области квантовых вычислений и машинного обучения в последние годы открывает новые главы в обсуждении этого вопроса.

Введение

Значительным шагом вперед здесь стала работа [1], посвященная практической демонстрации «квантового превосходства» – способности квантового компьютера решать некоторые задачи на порядок эффективнее классического вычислителя. Публикация указанной статьи тут же спровоцировала жаркую дискуссию и обострила важный практический вопрос: как существование квантового превосходства отразится на облике мира и на рынках? Для поиска ответа немного погрузимся в суть и историю квантовых вычислений.

Квантовый компьютер – это вычислительное устройство, использующее для обработки информации не двоичную логику, построенную на классических системах с двумя состояниями вроде транзистора «вкл/выкл», а аналогово-цифровой подход, в основе которого лежит хранение информации в квантовых двухуровневых системах. Такие элементарные ячейки квантовой информации получили название кубитов – по аналогии с битом, являющимся количеством информации в классической двухуровневой системе. Работа с информацией в таком виде имеет ряд особенностей, связанных с природой квантовой механики. Одни из них, например, способность кубита находиться в суперпозиции состояний 0 и 1 и, как следствие, возможность производить расчеты для множества наборов входных данных одновременно, существенно расширяют горизонты применения квантовых вычислителей. Другие же, такие как неизбежная потеря значительной доли информации при считывании, наоборот, ограничивают возможности такого рода программирования. И лишь грамотное построение алгоритмов, сочетающих положительные особенности для компенсирования отрицательных, позволяет при помощи квантовых компьютеров находить более эффективные подходы к решению ряда задач.

По-настоящему менять наше представление об облике мира в ближайшем будущем квантовые компьютеры начали тогда, когда с их помощью был открыт новый тип атак на классическую криптографию. Благодаря этому индустрия квантовых технологий за последние 30 лет развилась от интересной научной области до одного из самых перспективных технологических направлений. Уже в 2017 г. в отчете Объединенного исследовательского центра Европейской Комиссии констатируется существенный рост



количества ежегодно регистрируемых патентов в отрасли [2].

Более новое исследование [3] демонстрирует резкое увеличение числа стартапов в области квантовых вычислений после 2010 года. Ниже приведён график из данного исследования, отражающий рост числа компаний в области разработки квантово-вычислительного аппаратного обеспечения, вход в которую, вообще говоря, имеет довольно существенный порог.

Методы криптографии

Традиционно различают два класса криптографических схем: симметричные и асимметричные. В симметричных схемах отправитель и получатель сообщения используют общий секретный ключ, которым они либо обменялись заранее, либо использовали для его передачи другие криптографические методы. К схемам с секретным ключом относятся алгоритмы шифрования и имитозащиты, предназначенные для обеспечения конфиденциальности и целостности данных. В частности, по такому принципу работают блочные шифры «Кузнечик» и AES в режиме гаммирования или выработки имитовставки.

Асимметричные схемы в общем случае, напротив, не требуют заблаговременного обмена секретными ключами. Они используют два ключа: открытый и закрытый. Для начала взаимодействия одной из сторон достаточно передать второй стороне свой открытый ключ некоторым аутентифицированным образом, но при этом необязательно обеспечивать его конфиденциальность. Наиболее распространенными алгоритмами такого рода являются схемы электронной (цифровой) подписи и схемы согласования ключа. Последние применяются для выработки между взаимодействующими сторонами общего секретного ключа, который впоследствии может использоваться, в частности, при шифровании и имитозащите данных с помощью симметричных механизмов. Примерами схем согласования ключа являются механизмы на основе протокола Диффи – Хеллмана.

Кроме того, существуют криптографические примитивы, не использующие какие-либо ключи и играющие вспомогательную роль при защите. Типовым представителем этого класса является криптографическая хэш-функция, например «Стрибог» или SHA-3.

Симметричные криптографические механизмы применяются для защиты данных при передаче по открытым каналам или хранении. Масштабы и область применения защищаемых систем при этом могут быть самыми разными: от промышленных сетей и IoT до классических IP-сетей и высокоскоростных каналов между ЦОД; от локального хранения личных данных до удаленного хранения разветвленных баз и использования огромных облачных хранилищ. Асимметричные криптографические алгоритмы применяются при развертывании больших распределенных систем защиты, а также в сферах, требующих использования электронной подписи, например в системах электронного документооборота, в государственных и финансовых структурах. Для функционирования асимметричных механизмов, как правило, необходима довольно сложная инфраструктура, называемая PKI, неотъемлемой частью которой являются удостоверяющие центры (УЦ).

Криптографические хэш-функции применяются в связке как с симметричными, так и с асимметричными алгоритмами, например при диверсификации ключей, аутентификации, вычислении электронной подписи и т. д. В качестве отдельной технологии, активно использующей свойства криптографической хэш-функции, можно выделить блокчейн.

Стойкость большинства современных криптографических механизмов основывается на вычислительной сложности решения некоторой задачи. В случае симметричных механизмов такой задачей можно назвать нахождение ключа. Если атакуемый механизм является стойким, то наиболее эффективным подходом к решению этой задачи на классическом компьютере будет последовательный перебор. В случае асимметричной криптографии в основе каждого механизма может лежать своя вычислительная задача. Известными примерами являются задача факторизации – разложения целых чисел на простые множители и задача дискретного логарифмирования в поле вычетов или в группе точек эллиптической кривой. На сложности этих задач базируется стойкость всех распространенных практических асимметричных схем. Наконец, в случае криптографических хэш-функций выделяют задачу нахождения коллизии и задачу нахождения (второго) прообраза.

Каждая из перечисленных задач может быть решена на классическом компьютере. Количество действий, необходимых для решения задачи, – вычислительная сложность алгоритма. Выбирая параметры криптографической схемы, например длину ключа,

таким образом, чтобы наиболее эффективный известный алгоритм решения соответствующей задачи имел достаточно высокую сложность, мы получаем стойкую криптографическую схему.

Атака квантовым вычислителем на классическую криптографию

Важным свойством, объединяющим задачи, лежащие в основе асимметричных механизмов, является их однонаправленность – их сложно решить, но легко проверить решение. Более того, подобно случаю с поиском симметричного ключа, число действий, необходимых для взлома асимметричного шифра классическим компьютером, с увеличением ключа растет не пропорционально, а в разы. Это значит, что с появлением компьютера, способного взломать шифр за разумное время, достаточно будет лишь незначительно увеличить длину ключа, что вновь обеспечит стойкость схемы на годы вперед, пока компьютеры не станут в несколько раз мощнее.

Именно по такому свойству криптографических задач в 1994 г. смог ударить квантовый алгоритм Шора. Для него сложность разложения числа на простые множители с увеличением этого числа растет не в разы, а полиномиально. И если ключ шифра будет увеличен, квантовому компьютеру потребуется для взлома больше времени и памяти, но в обозримых масштабах. Исчезло преимущество криптографов в скорости наращивания сложности задачи, и теперь между ними и взломщиками стала возможна гонка, при переменном успехе в которой, естественно, нельзя будет говорить о сколько-нибудь надежной защите информации.

Еще одним чрезвычайно интересным квантовым алгоритмом является алгоритм Гровера. В это сложно поверить, но он позволяет находить в базе данных из N случайных элементов один нужный за $\sqrt{N}$ проверок, т. е. меньше, чем необходимо для простого обращения ко всем элементам базы. На самом деле никакого волшебства тут нет. В алгоритме Гровера лишь грамотно использована способность квантового компьютера обрабатывать информацию в некотором смысле параллельно, а считывание информации построено так, чтобы не разрушать полученные в ходе параллельной обработки полезные данные. Однако с классической точки зрения факт его работы остается удивительным, и его можно использовать для ускорения перебора симметричного ключа.

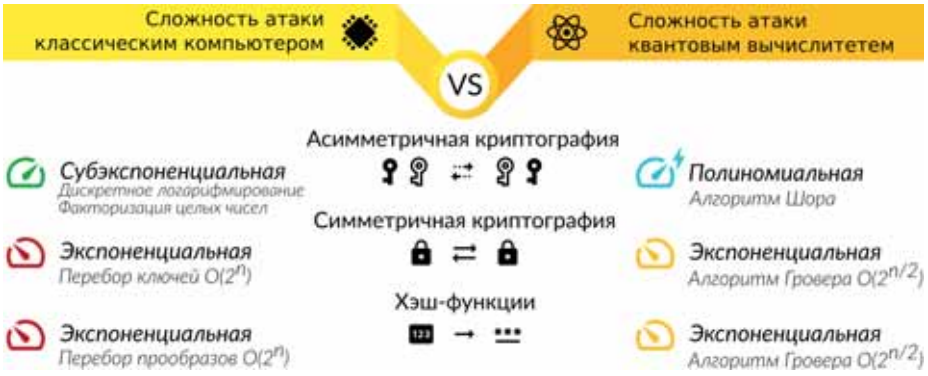
Алгоритмы Шора и Гровера создают прочный фундамент для ускорения решения многих криптографических задач. Подробные данные приведены в таблице.

Заметим, что алгоритм Гровера по сравнению с классической альтернативой не обеспечивает такого ускорения, как алгоритм Шора. Это означает, что появление достаточно мощного квантового компьютера потенциально окажет гораздо большее влияние на асимметричную криптографию, нежели на симметричную.

Исходя из схемы можно заключить, что появление квантового компьютера приведет к необходимости:

- для хэш-функций: увеличения длины хэш-кода в два-три раза;
- для симметричных механизмов: увеличения длины ключа в два раза;
- для асимметричных механизмов: экспоненциального увеличения длины ключей.

Для симметричной криптографии и хэш-функций двух-трехкратное увеличение длины ключей и хэш-кодов не является критичным. Даже сейчас существуют и применяются на практике симметричные механизмы и хэш-функции, удовлетворяющие новым, «квантовым» критериям стойкости. Совсем иная ситуация с асимметричными механизмами. Для них потребуется экспоненциальное увеличение длин параметров, что сделает, по сути, невозможным их применение на практике.



Квантовая и постквантовая криптография

Очень символично, что в области квантовых технологий лежат и щит, и меч для информационной безопасности. Квантовая физика дала нам компьютер, потенциально способный разрушить классическую криптографию. Она же дает нам квантовую криптографию – способ защитить информацию даже от квантового компьютера.

Первым протоколом квантовой криптографии стал BB-84, предложенный Чарльзом Беннетом и Жилем Брассаром в 1984 г. Опишем его работу для оптических кубитов. Свет, будучи электромагнитной волной, характеризуется ориентацией плоскости, в которой лежит волна – поляризацией. Её считывание зависит от выбора базиса измерений – фотон вертикально поляризованного света всегда пройдёт проверку на вертикальную поляризацию и никогда

на горизонтальную. Но при поляризации под 45° фотон пройдёт эти проверки с равным шансом. При этом после измерения информация теряется – фотон оказывается в состоянии, проверку на которое прошел успешно.

BB84 использует два базиса – вертикально-горизонтальный и ±45°. Отправляемое состояние выбирается случайно. Получатель же случайно выбирает базисы для серии измерений. После этого получатель открыто называет отправителю использованные базисы и узнаёт, в каких измерениях он ошибся. Их результаты отбрасываются, остальные же формируют секретный ключ. При попытке перехвата, состояния фотонов будут нарушаться, что приведёт к появлению ошибок в канале связи. Если изначально канал был достаточно малошумный, факт прослушки будет зафиксирован.

Подобные протоколы квантовой криптографии позволяют быстро вырабатывать секретные ключи для последующего использования стойкой симметричной криптографией, что сводит на нет даже угрозу атаки квантовым вычислителем.

В целом методы противодействия атакам квантового компьютера можно разделить на два класса. К первому относятся механизмы, обладающие теоретико-информационной стойкостью, например одноразовый блокнот, семейство универсальных хэш-функций и упомянутое квантовое распределение ключа. Они позволяют обеспечить защиту вне зависимости от вычислительных возможностей противника. Второй класс образуют классические методы, называемые алгоритмами постквантовой криптографии.

В основе постквантовой криптографии лежит поиск математических задач, для которых на текущий момент неизвестен эффективный алгоритм решения ни на классическом, ни на квантовом компьютере. К разделам математики, потенциально содержащим такие задачи, относятся теория решеток, теория кодирования, изогении на эллиптических кривых и т. д. На основе этих задач строятся новые асимметричные криптографические схемы, стойкие к атакам квантового компьютера, в частности схемы электронной подписи и схемы согласования ключа.

В настоящее время активно ведется разработка постквантовых асимметричных схем. Как и в случае с любыми другими криптографическими алгоритмами, важным шагом на пути к их широкому практическому использованию является их стандартизация. В 2017 г. NIST инициировал конкурс PQC, ставящий своей целью выбор наиболее перспективных постквантовых схем с последующей стандартизацией. На текущий момент идет третий, заключительный раунд конкурса. Некоторые из постквантовых механизмов уже стандартизованы в документах ANSI, IEEE, IETF. Параллельно работы ведутся и в России: в рамках РГ 2.5 ТК 26 исследуются вопросы синтеза и анализа постквантовых схем в целях их стандартизации.

Тем не менее практическое применение постквантовых механизмов «здесь и сейчас» сопряжено с рядом проблем как технического, так и организационного характера. Как правило, такие механизмы являются менее эффективными с точки зрения эксплуатации по сравнению с их классическими аналогами. Это может выражаться в более низкой производительности и/или в больших размерах данных, например ключей, шифртекстов, подписей. В связи с относительной новизной направления многие из предлагаемых схем являются слабо исследованными, что несет в себе определенные риски их использования. Отдельной сложной задачей является организация массового повсеместного перехода на постквантовые алгоритмы. Такой переход потребует перестройки всех действующих PKI и затронет работу огромного количества УЦ, что повлечет за собой ощутимые временные и финансовые затраты.

Пожалуй, самым важным аспектом является то, что ни для одной существующей постквантовой схемы криптографическая стойкость не является строго доказанной. Нет оснований полагать, что не будут открыты квантовые, а может быть, даже и классические алгоритмы, эффективно решающие математические задачи на основе этих схем. А с учетом описанных технических сложностей внедрение постквантовой криптографии начинает в ряде случаев по привлекательности соперничать с использованием симметричной криптографии с квантовым распределением ключей, внедрение которой бесспорно будет технически более сложным, зато гарантированно обеспечит криптографическую стойкость канала связи в будущем.

Перспективы квантовых вычислений

Вернемся к вопросу квантовых вычислителей. Если уже более 20 лет существует алгоритм Шора, ставящий под угрозу существующие методы защиты информации, то почему классической криптографией до сих пор пользуются? Дело, как нетрудно догадаться, в несовершенстве квантовых вычислителей. Помимо того, что в криптографии используются достаточно «длинные» ключи и доступного объема кубитных регистров (см. рисунок) пока в принципе недостаточно для их взлома, квантовые компьютеры еще и подвержены возникновению ошибок в процессе вычислений. Противодействовать этому призваны методы коррекции, которые, однако, требуют использования еще большего количества кубитов.

Вопрос количества кубитов и ошибок вычислений отсылает нас к аппаратным архитектурам квантовых вычислителей. Легче всего этот вопрос решается для систем на основе линейно-оптических чипов. Инертность фотонов теоретически позволяет наращивать объем регистра до тысяч и даже миллионов

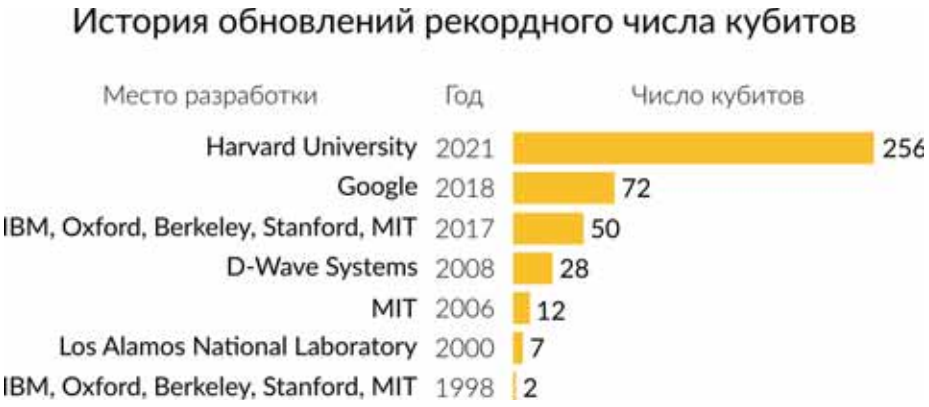


Рисунок. *Рост количества кубитов со временем*

кубитов. Но отсюда же следует и недостаток: реализация взаимодействия фотонов в многокубитных операциях, необходимых для построения универсального вычислителя, становится настоящей проблемой, требующей подчас весьма оригинальных инженерных решений.

В обратной ситуации находятся квантовые компьютеры на основе сверхпроводящих схем. Именно эта архитектура сегодня наиболее распространена. Сверхпроводящими кубитами удобно манипулировать, но они очень подвержены влиянию шумов, что ограничивает объем кубитного регистра.

Сбалансированный подход предоставляют архитектуры на основе ионов и атомов в оптических ловушках. Реализация методов подавления ошибки для атомного регистра недавно позволила реализовать вычислитель с 256 кубитами, что является рекордом на сегодня [3]. В свете того, что развитие сверхпроводящих схем столкнулось со значительными трудностями на отметке в 50 кубитов, а крупный квантовый вычислитель на основе оптических схем остается пока в области долгосрочных перспектив, не исключено, что именно реализация на основе атомов в ловушках станет доминирующей архитектурой квантовых вычислителей в ближайшие 5–10 лет и именно такого типа компьютер первым доберется до объема регистра порядка 1000–10 000 кубитов, что создаст уже вполне реальную угрозу для классических систем защиты информации. В России разработкой вычислителя с таким типом аппаратной архитектуры, а также с архитектурой на основе линейной оптики занимается Центр квантовых технологий МГУ имени М.В. Ломоносова.

В целом, несмотря на отсутствие сегодня квантового вычислителя достаточной мощности, последствия его появления следует принимать в расчет уже сейчас. В первую очередь это обусловлено самой спецификой сферы информационной безопасности, которая подразумевает необходимость защиты данных в течение определенного промежутка времени. Срок, на который данные должны быть защищены, может определяться различными факторами, в том числе и весьма субъективными. Интерес в данном случае представляет соотношение даты окончания срока защиты конкретных данных и даты появления полноценного квантового компьютера. Если второе событие произойдет раньше, то информация будет под угрозой. Как следствие, она с самого начала должна быть защищена методами, стойкими к атакам квантового компьютера.

Кроме того, нужно принимать во внимание тот факт, что переход на новые криптографические механизмы или на принципиально новые технологии защиты происходит не мгновенно и, как правило, растянут во времени. Учитывая, что системы защиты должны функционировать уже к моменту начала защиты данных, об их разработке и внедрении необходимо задумываться еще более заблаговременно.

Заключение

В то время как вопрос со стандартизацией и широким внедрением постквантовых алгоритмов пока висит в воздухе, технология квантового распределения ключей активно совершенствуется и уже вышла на уровень практических применений. В России ведутся исследования возможностей и влияния квантовых вычислений на криптографические средства, а несколько компаний – вендоров в области защиты информации – работают над созданием собственных систем квантового распределения ключей. В частности, системы ViPNet Quandor и ViPNet Quantum Security System уже технологически готовы к промышленной эксплуатации и находятся на этапе сертификационных испытаний. Также в настоящий момент сразу несколько отечественных компаний и ведущих вузов страны занимаются квантовыми разработками. Значение научных исследований и практических разработок в этой сфере огромно, так как активное развитие подобных систем позволит обеспечить защиту информации, даже в условиях появления эффективного квантового компьютера. ■

Литература

1. *Arute F., Arya K., Martinis John M. и др. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574, 505–510.*
2. *Travagnin M. Patent analysis of selected quantum technologies. JRC Technical Reports, 2019.*
3. *Sepehr Ebadi, Tout T. Wang, Mikhail D. Lukin и др. Quantum phases of matter on a 256-atom programmable quantum simulator. Nature volume, 2021, 595, 227–232.*