Квантовая криптографическая катастрофа. Часть 1

Виктор Алексеев (victor.alexeev@gmail.com)

В конце 2001 года в журнале «Nature» была опубликована статья с описанием эксперимента, подтверждающего реальную возможность проведения факторизации больших чисел с помощью квантового компьютера. Эта новость, воспринятая как предупреждение о том, что любые криптографические шифры могут быть легко взломаны с помощью квантового компьютера, мгновенно облетела все научные и популярные издания мира. Во всех странах началась паника. Однако за 21 год, прошедший со времени этой публикации, квантовый релевантный компьютер (CRQC), способный взламывать криптографические шифры, не был создан. Никто точно не может предсказать, когда это может произойти. Несмотря на огромные технические проблемы, постоянно возникающие перед разработчиками, направление квантовых компьютеров интенсивно развивается.
В статье описаны основные этапы развития CRQC и показана эволюция самой схемотехнической идеи квантового релевантного компьютера. На заре своего появления первоначальная схема CRQC предполагала использование универсального цифрового квантового компьютера с вентильной обработкой типа IBM-Q. Спустя двадцать лет были разработаны новые технологии, позволяющие реализовать процессы факторизации с помощью других устройств, таких как вариационный квантовый вычислитель собственных значений, вариационный решатель с квантовым отжигом и решатель на базе квантового отжига со встроенным умножителем факторинга. Если в будущем появятся гибридные облачные платформы, объединяющие мощные стандартные компьютеры и специализированные квантовые вычислители разного типа, то возникновение CRQC может наступить раньше, чем его ожидают. В качестве средства борьбы с CRQC сегодня интенсивно разрабатываются системы «постквантовой криптографии».
В предыдущих статьях, опубликованных в журнале (№ 7, 8, 9 за 2022 год), были описаны типы современных квантовых компьютеров, принципы их работы, а также приведено объяснение используемых терминов и аббревиатур.

Угроза квантового апокалипсиса

В прошлом году мир отметил двадцатилетнюю годовщину начала квантовой войны с криптографическими системами. В конце декабря 2001 года в журнале «Nature» появилась статья «Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance», посвящённая экспериментальному подтверждению работоспособности алгоритма Шора для проведения факторизации больших чисел с помощью квантового компьютера [1].

Эта новость, воспринятая как предупреждение о том, что асимметричные криптографические системы с открытым ключом могут быть легко взломаны с помощью квантового компьютера, мгновенно облетела все научные и популярные издания мира, вышедшие под заголовками, похожими на «квантовый компьютер – это страшнее атомной бомбы».

Асимметричное шифрование подразумевает тот факт, что посторонним лицам может быть известен алгоритм шифрования, а также открытый ключ, но неизвестен закрытый ключ, который знает только получатель. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), а также SSH, PGP, S/MIME и других.

На данный момент асимметричное шифрование на основе открытого ключа, получившее название «RSA», используется в большинстве продуктов на рынке информационной безопасности [2]. Этот протокол шифрования был разработан фирмой RSA, являющейся одной из ведущих в мире организаций, специализирующихся на криптографических системах [3].

Простейшая формула ассиметричного кода с открытым ключом чрезвычайно проста: передающая и принимающая стороны знают два сомножителя большого числа.

В упрощённом виде для того, чтобы взломать код, нужно всего лишь на вход компьютера подать составное число N в двоичной записи, а на выходе получить два простых числа p и q, такие, что $N = pq$. Нужно перебрать весь мыслимый диапазон значений числа N и получить ключи к шифру. Всё просто для небольших значений N.

Однако современные длинные пары ключей содержат так называемые «большие числа». К числу «больших чисел», в частности, относятся RSA-числа [4].

Например, 2048-битная реализация протокола RSA соответствует ключу длиной 617 десятичных цифр. Если пытаться искать простые сомножители этого числа методом перебора, то даже при использовании самых современных компьютеров с бинарной логикой на это потребуются сотни тысяч лет (рис. 1). Наилучшие из известных классических детерминированных алгоритмов факторизации для стандартных компьютеров с бинарной логикой не позволяют решать подобные задачи.

В современной математике есть разделы, которые относятся к классу сложных задач. Они не могут быть решены с помощью современных стандартных цифровых компьютеров с двоичной логикой за «разумное полиномиальное время». К классу таких задач относится так называемая факторизация «больших чисел», которая неразрывно связана с проблемами криптографической безопасности. Достаточно подробно и квалифицированно эти вопросы рассмотрены в публикации [6]. Не сосредотачиваясь на математических деталях пробле-

мы, отметим только основные моменты алгоритма Шора и важность его практической реализации с помощью квантовых компьютеров с вентильным управлением. Составные числа, в принципе, можно разложить на простые множители с помощью алгоритма Шора и квантового компьютера, но не абсолютно точно, а лишь с некоторой вероятностью.

С разложением чисел на простые множители, которое в математике называется факторизацией, всё действительно просто для относительно небольших значений N. Однако для больших значений N факторизация даже и в настоящее время представляет заметную проблему современной математики [6].

Для того чтобы привлечь к решению проблемы максимальное число математиков со всего мира, в 1991 году был объявлен конкурс «RSA Factoring Challenge», который официально закончился в 2007 году. В рамках этого конкурса были разложены на простые множители числа вплоть до RSA-768, длиной 768 бит. На разложение этого числа потребовалось почти два года (2007–2009) непрерывной работы сотен мощных стандартных компьютеров с бинарной логикой [7, 8].

В феврале 2020 был завершён рекордный процесс факторизации числа «829-bit RSA». Эти вычисления были выполнены с помощью объединения огромных вычислительных мощностей цифровых компьютеров с двоичной логикой на базе Intel Xeon Gold 6130 при использовании алгоритма Number Field Sieve и программного обеспечения CADO-NFS с открытым исходным кодом.

Общее время вычислений составило примерно 2700 PCY. Термин «PCY – physical core-years» означает эквивалент времени, при котором ЦПУ с одним ядром использовалось непрерывно в течение года [9].

Поскольку современные цифровые компьютеры с двоичной логикой не могут решить задачу для больших чисел за «разумное, полиномиальное время», то факторизация в настоящее время затормозилась в ожидании появления новых вычислительных технологий, среди которых наиболее реальной является идея использования квантового компьютера с вентильным управлением и алгоритма Шора для ускорения процесса факторизации больших чисел [10].

В предыдущих статьях, опубликованных в журнале СоЭл [11, 12, 13], было отмечено, что в конце 1990-х годов в научном мире стало приходить понимание принципиальной невозможности создания универсального квантового цифрового компьютера, способного взламывать любые шифры на базе существующих технологий. Для этого необходим был бы квантовый компьютер, содержащий десятки тысяч кубитов. Основным непреодолимым препятствием появления такого устройства стали шумы и проблемы декогерентности квантовых компьютеров с вентильной обработкой.

В дальнейшем направление квантовых компьютеров стало развиваться по трём основным сегментам [14, 15]:

- совершенствование технологий универсальных квантовых цифровых компьютеров с вентильной обработкой (Universal Digital Quantum Gate Computer UDQGC);
- разработка и производство адиабатических вычислителей с квантовым отжигом (Quantum Annealing Processing Unit – QAPU);
- разработка криптографически релевантного квантового компьютера (Cryptographically Relevant Quantum Computer – CRQC).

В эти годы по всему миру стали появляться проекты создания так называемого «криптографически релевантного квантового компьютера» (Cryptographically Relevant Quantum Computer – CRQC), способного взламывать существующие шифры [14].

На волне паники возникло огромное количество «экспертов» по квантовой физике, которые сходились на том, что с помощью алгоритма Шора теоретический идеальный универсальный квантовый компьютер с вентильной обработкой UQGC способен достаточно быстро взламывать большинство используемых тогда асимметричных криптографических схем. Ключевое слово здесь было «идеальный». Но, как оказалось, для достижения этого свойства «идеальности» конструкторам квантового компьютера нужно было преодолеть огромные научные и технологические проблемы, с которыми учёные раньше не сталкивались [15…17]. Например, для того чтобы взломать 256-битный шифр за один день, потребуется универсальный квантовый компьютер современного технологического и научного уровня, но содержащий около 13 миллионов кубитов. Для сравнения стоит напомнить, что самый мощный из существующих на сегодняшний день квантовых процессоров – IBM Osprey – имеет всего лишь 433 работоспособных кубита [18].

Рис. 1. Для разложения числа 2048-RSA на простые множители с помощью стандартного компьютера с бинарной логикой потребуются сотни тысяч лет непрерывной работы [5]

Экспериментальное подтверждение возможности использования квантового компьютера для факторизации больших чисел

В опубликованной в 2001 году в журнале «Nature» статье были приведены результаты первого эксперимента по разложению на множители больших чисел, проведённого с помощью одной из ранних моделей цифрового квантового компьютера типа UDQGC с вентильным управлением [1].

В этой работе объединённая группа учёных из исследовательского центра IBM Almaden Research Center и университета Stanford University экспериментально доказала возможность реализации квантового алгоритма факторинга Шора на простейшем примере разложения числа 15 на простые множители.

Напомним, что этот алгоритм демонстрирует теоретическую возможность целочисленной факторизации больших чисел с помощью квантовых вычислений.

Алгоритм Шора представляет собой квантовый алгоритм, позволяющий находить за полиномиальное время с высокой вероятностью множители нечётного составного целого числа $N = pq$.

В общем случае алгоритм Шора включает в себя четыре основных этапа:

- выбор случайного остатка числа «*a*» по модулю **N**;

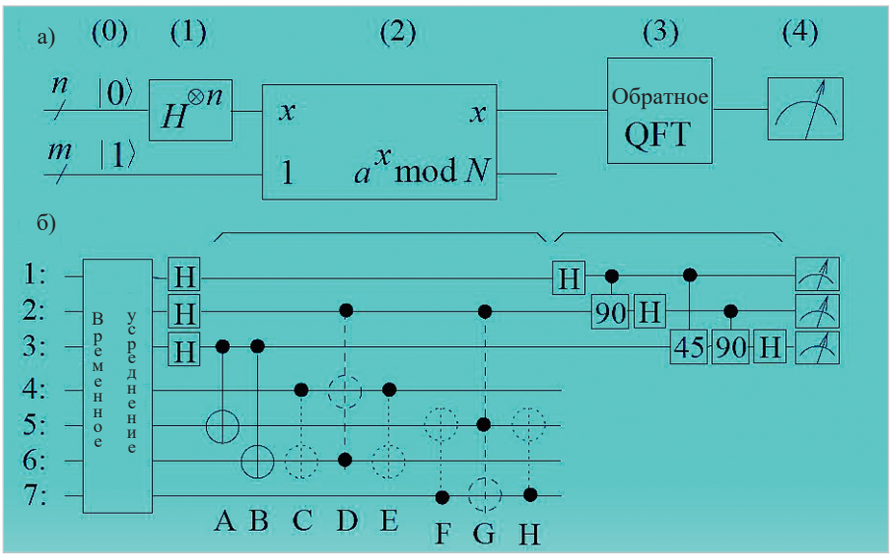

Рис. 2. Схема оригинального эксперимента по факторизации числа «пятнадцать» с помощью квантового компьютера и алгоритма Шора [1]

- проверка наибольшего общего делителя с помощью выражения **НОД(a,N) = 1**;
- определение порядка r остатка a по модулю **N**;
- вычисление **НОД($a^{r/2}$−1,N)** в случае, если порядок r является чётным числом.

Следует иметь в виду, что минимальное значение r, при котором a в степени r тождественно равно единице (**mod N**), называется порядком a по модулю **N**. Именно в этом смысле в дальнейшем будет употребляться термин «порядок» (order). Порядок r является периодом функции $\mathbf{f}(x) = a^x \mathbf{mod\ N}$.

Наиболее трудным этапом в реализации квантового алгоритма Шора является как раз определение порядка a по модулю **N**.

В этом эксперименте использовались спиновые кубиты на базе молекул C_4F_5Fe (perfluorobutadienyl iron) с изотопом углерода C13. Лабораторный образец квантового компьютера с ядерным магнитным резонансом позволил реализовать простейший пример факторизации числа «пятнадцать» (15 = 3 × 5) с помощью алгоритма Шора. Следует подчеркнуть, что семь кубитов не позволяли реализовать факторизацию следующего числа без увеличения количества кубитов, что в те времена и при данной конструкции квантового компьютера не представлялось возможным.

Схема оригинального эксперимента по факторизации числа «пятнадцать» с помощью квантового компьютера и алгоритма Шора показана на рис. 2.

Идея эксперимента заключалась в том, чтобы с помощью универсального квантового компьютера с вентильной обработкой (UDQGC) при использовании квантового преобразования Фурье (Quantum Fourier Transform – QFT), дискретного логарифма (Discrete logarithm – DL) и оператора Адамара (Hadamard operator – H) последовательно перебирать возможные варианты искомых сомножителей, следуя перечисленным выше шагам алгоритма Шора.

В квантовом алгоритме Шора используется известная процедура квантовой оценки фазы (Quantum Phase Estimation – QPE), а также последующее определение собственного значения для некоторой унитарной матрицы U, соответствующего собственному вектору |u⟩. Задача факторизации при этом сводится к нахождению за полиномиальное время количества битов, целевого числа, порядок которого определяется логарифмом $\log_2 N$. Решив задачу поиска порядка целевого числа с помощью QPE и выполнив несколько дополнительных шагов, можно уже дальше разложить на множители целое число N. В настоящее время неизвестен алгоритм, способный решить эту задачу для «больших чисел» за полиномиальное время с помощью стандартного цифрового компьютера с бинарной логикой SBLC (Standard Binary Logic Computer) [19].

В верхней части на рис. 2 схематически показаны основные этапы эксперимента в соответствии с алгоритмом Шора. В нижней части на рис. 2 приведена детальная квантовая схема эксперимента для числа N = 15 и количества кубитов a = 7.

На рис. 2 квадратиками обозначены вентили определённых операторов. Например, «**H**» – оператор Адамара, а «**45**» и «**90**» – это унитарные гейты вращения кубитов.

Операция QFT (Quantum Fourier Transform) позволяет разложить заданную матрицу в произведение более простых унитарных матриц. Оператор Адамара используется в качестве разделителя кубита на его возможные состояния. Решение задачи ищется в форме дискретного логарифма. Функцию HD выполняют соответствующие вентили (Hadamard quantum gate – **H**). Фактически оператор **H** разделяет кубит на равновероятные состояния. Например, если кубит соответствовал состоянию ноль, то H переведёт его в суперпозицию между нулём и единицей. После окончания процесса в тот момент, когда будет производиться измерение кубита, он случайным образом может оказаться как в нуле, так и в единице.

Функционально квантовый процесс вычислений состоит из четырёх последовательных этапов, включающих задание начального состояния термического равновесия для семи кубитов, дискретное логарифмирование, квантовое преобразование Фурье, измерение конечных состояний.

В соответствии с алгоритмом Шора, в котором рассматриваются только чётные порядки, инициализация начиналась со значения первого регистра, равного $n = \mathbf{2[\log_2 N]}$ (где n – количество кубитов, **N** – целевое число процесса факторизации). Во второй регистр записывалось значение $m = \mathbf{2[\log_2 N]}$ и т.д. На следующем этапе оператор Адамара применялся к первым «n» кубитам. Далее второй регистр умножался на функцию $\mathbf{[f(}x\mathbf{) = } a^x \mathbf{\bmod N]}$, где a < N не имеет общих множителей с N. Затем выполнялось обратное квантовое преобразование Фурье (**QFT**) на первом регистре. На последнем четвёртом этапе проводилось измерение состояний первого регистра.

Необходимо особо подчеркнуть, что в использованной схеме перебора значений для реализации операции **QFT** необходимо такое количество вентилей **H**, которое будет кратно квадрату количества вычислительных кубитов (n^2). При использовании стандартного компьютера с двоичной логикой для разложения числа в ряд с помощью преобразования Фурье потребуется количество управляемых ячеек памяти, кратное

2^n, что экспоненциально больше, чем количество квантовых вентилей Адамара (**H**), необходимых для операции квантового преобразования Фурье QFT с помощью квантового UDQGC. Благодаря тому, что кубиты имеют три возможных состояния и обладают свойством квантовой запутанности, а кроме того, изменения их квантовых состояний происходят практически мгновенно и параллельно, использование квантового UDQGC позволяет многократно увеличить скорости вычисления в задачах, решаемых методом перебора, по сравнению со стандартными компьютерами с двоичной логикой SDCBL.

В то же время следует отметить хорошее совпадение между измеренными и смоделированными спектрами, которое продемонстрировало надёжность полученных результатов и перспективность работ в данной области. Подробно пример разложения числа 15 на простые множители с помощью современного компьютера IBM рассмотрен на сайте [20].

Сегодня пример разложения числа «15» на простые множители может повторить любой желающий самостоятельно в онлайн-режиме с использованием симулятора современного квантового компьютера IBM и усовершенствованных алгоритмов обработки [21]. Однако двадцать лет назад результаты работы авторского коллектива учёных и инженеров в составе *Ливена Вандерсипена (Lieven M.K. Vandersypen), Матиаса Штеффена (Matthias Steffen), Грегори Брейта (Gregory Breyta), Костантино С. Яннони (Costantino S. Yannoni), Марка Х. Шервуда (Mark H. Sherwood) и Исаака Л. Чуанга (Isaac L. Chuang)* вызвали ошеломляющий эффект во всём мире. Этот эксперимент, доказавший возможность практического использования квантового компьютера для факторизации больших чисел с помощью ранее опубликованного теоретического протокола Шора, стал краеугольным камнем данного направления. Кроме того, в этой работе были сделаны выводы о значении декогеренции кубитов как основного источника ошибок, ограничивающих вычислительные возможности квантового компьютера с вентильным управлением.

Во многом шокирующий эффект статьи был спровоцирован первыми комментариями околонаучных таблоидов и слухами о грозящем крахе секретности любых шифров. Практически в первые годы после этой публикации во всех развитых странах мира началось невиданное финансирование научных проектов, связанных с квантовыми компьютерами. Первые успехи использования квантового компьютера для разложения чисел на простые множители стали мощным стимулом того, что в разных концах света как грибы после дождя начали появляться сотни новых лабораторий, которые с огромным энтузиазмом взялись за развитие квантовых вычислений. Начался поиск путей создания так называемого «криптографически релевантного квантового компьютера» (Cryptographically Relevant Quantum Computer – CRQC), способного взламывать шифры с открытым кодом.

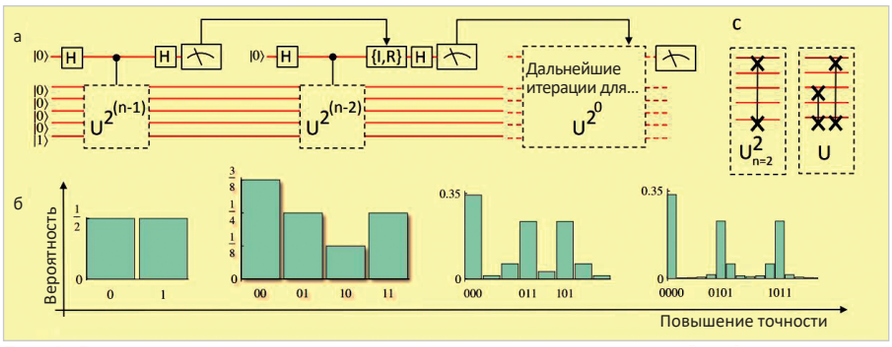

Рис. 3. Схема квантового алгоритма итеративного поиска порядка факторизации числа двадцать один [21]

В дальнейшем концепция CRQC развивалась по двум направлениям. С одной стороны, разрабатывались чисто технические вопросы кубитов и квантовых компьютеров. С другой, продолжались поиски новых квантовых алгоритмов, необходимых для факторизации больших чисел.

В 2012 году была предложена концепция алгоритма факторизации целого числа 21, в которой вместо схемы последовательного перебора использовалась итеративная схема [22].

На рис. 3 приведена схема алгоритма итеративного поиска порядка факторизации числа двадцать один. Квадратиками на рис. 3 обозначены соответствующие квантовые логические вентили (H, R, U, I).

В использованной итеративной версии алгоритма поиска порядка числа (iterative version of the order finding algorithm) регистр управления содержит только один кубит. В процессе вычислений этот кубит повторно и многократно используется n раз. При этом на каждой итерации реализуются измерения и новые настройки параметров. Такой метод обеспечивает дополнительный бит точности.

В этой работе итерационная версия алгоритма нахождения порядка вместо одновременного выполнения преобразования Фурье для всех кубитов регистра управления использует измерение когерентности между вычислительными базисными состояниями отдельных кубитов в регистре управления. Измерение управляющего кубита после каждого контролируемого унитарного числа даёт следующий старший бит на выходе, и результат передаётся на итерированное (квазиклассическое) преобразование Фурье, которое применяет либо тождественную операцию **I**, либо соответствующий фазовый вентиль **R**, предшествующий Адамару **H**. В зависимости от предыдущего результата вычислений, переход к следующему этапу определялся с учётом фазовой когерентности следующего измерения.

При таком подходе управляющий регистр не может обслуживать более одного кубита одновременно. Все унитарные операции, контролируемые i-м управляющим кубитом, выполняются раньше, чем операции, которые обусловлены (i+1)-м управляющим кубитом. Таким образом, операции с i-м кубитом могут быть выполнены до того, как будет инициализирован (i+1)-й кубит. Поэтому один управляющий кубит может быть использован повторно. При этом состояние рабочего регистра обновляется на каждом новом этапе итераций.

Как видно из рис. 3 (б), чем больше число итераций, тем выше точность. Итерационный метод позволяет в принципе значительно сократить количество рабочих кубитов за счёт уменьшения количества управляющих кубитов. Однако по мере уменьшения количества управляющих кубитов или итераций n точность вычислений

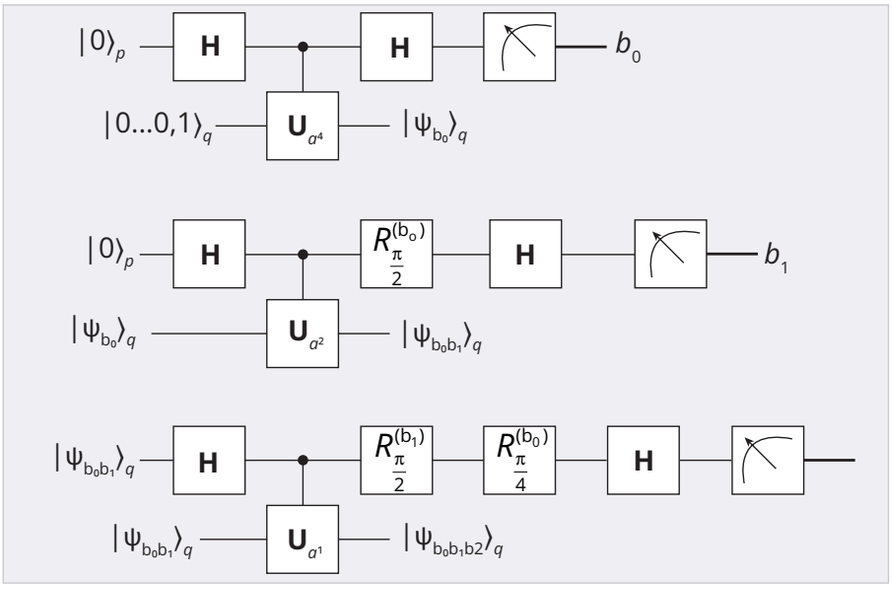

Рис. 4. Схема факторизации чисел 15, 17, 35 на квантовом процессоре ibmqx5 с использованием модифицированного алгоритма Шора [23]

снижается, и пики k в распределении вероятностей становятся размытыми, как это показано на рис. 2 (б). Однако в случае, когда порядок равен степени числа два и $r = 2p$, пики вероятностей точно соответствуют логическим состояниям кубитов.

Необходимо подчеркнуть, что в этой работе была продемонстрирована только принципиальная возможность самого метода с использованием лабораторного макета кубитов. Фактически процесса факторинга как такового здесь не наблюдалось из-за небольшого количества итераций.

Первоначальная идея CRQC заключалась в использовании алгоритма факторизации именно на универсальном квантовом компьютере с вентильной обработкой. В этом смысле подобный эксперимент был проведён только в 2019 году, когда стал доступен компилятор IBM лидера группы квантовых вентильных компьютеров типа UDQG.

Для факторизации чисел 15, 21 и 35 на квантовом процессоре IBM в этой работе были применены итеративная схема и метод объединения результатов [23].

В качестве аппаратной части был задействован квантовый процессор «IBM ibmqx5» с шестнадцатью сверхпроводящими кубитами, распределёнными на плоскости в виде двух соседних массивов по восемь штук в каждом. Схема факторизации чисел 15, 21, 35 на квантовом процессоре ibmqx5 с использованием модифицированного алгоритма Шора показана на рис. 4.

Практически в этом эксперименте использовался гибридный алгоритм, согласно которому вся схема разделена на три составные части. Каждая схема содержит отдельный этап модульной обработки и измерения состояния регистров каждого периода. Объединение этих отдельных этапов реализовано с помощью классического алгоритма. При этом сначала определяется квантовое состояние вычислительного регистра в конце предыдущей схемы, которое затем передаётся в качестве входных данных на следующий контур. Такая гибридная схема снижает ресурсоёмкость алгоритма за счёт выполнения частей задачи оптимизированными способами и факторизации задачи в целом на основе алгоритма Шора.

Идея разбиения общей задачи факторизации на мелкие фрагменты с последующей обработкой каждого из них по отдельности наиболее эффективным способом была реализована с использованием метода «вариационного квантового вычислителя собственных значений» (Variational Quantum Eigensolver – VQE). Этот квантовый вычислитель мы рассмотрели в предыдущем номере журнала [24].

Вариационный квантовый вычислитель собственных значений (VQE) был разработан специально для получения вероятностных оценок основных состояний (eigensolvers) сложных квантовых систем с использованием вариационного метода (variational) на базе универсальных цифровых вентильных квантовых компьютеров (UDGQC) и стандартных цифровых компьютеров с двоичной логикой (SBLC) [25].

Основным назначением VQE было решение оптимизационных задач методом вариационного поиска основных состояний квантовой системы. Особо следует подчеркнуть, что метод VQE был разработан для квантовых логарифмов, предназначенных для решения трудных задач типа NP, таких, например, как модель Изинга. Наиболее подробно VQE-метод описан в одной из последних публикаций 2022 года [26].

Вариационные квантовые решатели основных состояний (VQE) фактически представляют собой симбиоз классического и квантового компьютеров. При этом роли между ними распределяются следующим образом. Стандартный компьютер с бинарной логикой (SBLC) производит градиентный поиск в пространстве всех возможных аргументов функций, для которых нужно найти основные состояния или, говоря другими словами, минимальные значения гамильтониана. В свою очередь, квантовый компьютер (UDGQC) определяет мгновенные значения гамильтониана системы и находит с некоторой вероятностью его основное (наименьшее) значение.

Одним из основных моментов в теории VQE является хорошо известный «вариационный метод», который позволяет упростить сложную задачу на начальном этапе её решения с целью получения некоего начального оценочного результата. Вместо задачи с многочисленными неизвестными варьируемыми параметрами в качестве первого пробного варианта используют какую-нибудь упрощённую функцию с небольшим количеством параметров. При этом ожидаемое значение гамильтониана, вычисленного в пробном состоянии, оценивается в рамках VQE как целевая функция. Шаг за шагом, варьируя параметры, на каждом из следующих этапов вычислений получают результат, максимально соответствующий искомой функции.

Как правило, опытному специалисту, знакомому с предметом, удаётся найти такие простые подстановочные функции (ansatz), которые позволяют успешно аппроксимировать минимальное значение гамильтониана.

Таким образом, упрощённый процесс вычислений с помощью VQE можно представить как разделение ролей между стандартным и квантовым ком-

пьютерами. Стандартный классический компьютер с двоичной логикой (SCBL) определяет пробную функцию (ansatz) и характеризующие её параметры.

Затем этот классический компьютер связывается через соответствующий интерфейс с одним из универсальных цифровых квантовых компьютеров с вентильным управлением (UDGQC), который вычисляет с определённой долей вероятности мгновенные значения гамильтониана в заданных промежуточных точках. Вычисленные значения возвращаются обратно на стандартный компьютер SCBL в виде классических битовых строк. Это взаимодействие может быть итеративным. В таком варианте стандартный компьютер SCBL периодически посылает сигналы связи и управления квантовому компьютеру, например, предлагая новые значения параметров для использования в параметризованной квантовой схеме.

Пробная эвристическая функция «ansatz» (анзац), имеющая несколько параметров, позволяет варьировать её поведение в широком диапазоне. Зная, что, хотя бы примерно, хотелось бы получить на выходе, можно на основе имеющегося опыта предположить, какого именно типа целевую функцию следует искать. Чем точнее первое предположение (ansatz), тем удачнее будет окончательное решение.

Нужно напомнить, что современные универсальные цифровые компьютеры с вентильным управлением представляют собой грандиозные технические сооружения, оснащённые мощными криогенными установками и сложнейшей электроникой. Эти уникальные устройства стоимостью сотни миллионов долларов могут позволить себе поддерживать и развивать лишь несколько индустриальных гигантов в мире, таких как IBM, Google, Microsoft's Azure Quantum.

Продолжение статьи читайте в следующем номере журнала.

Литература

1. URL: https://www.nature.com/articles/414883a
2. URL: https://e-nigma.ru/stat/rsa/
3. URL: https://www.rsa.com/company/
4. URL: https://ru.wikipedia.org/wiki/RSA-%D1%87%D0%B8%D1%81%D0%BB%D0%B0
5. 5URL: https://www.istockphoto.com/photos/dance-floor-texture
6. URL: https://www.researchgate.net/publication/330369215_Factorising_large_numbers
7. URL: https://eprint.iacr.org/2010/006.pdf
8. URL: https://ru.wikipedia.org/wiki/RSA-%D1%87%D0%B8%D1%81%D0%BB%D0%B0
9. 9URL: https://ec.europa.eu/eurostat/ramon/cybernews/abbreviations.htm
10. URL: http://mmrc.amss.cas.cn/tlb/201702/W020170224608150589788.pdf
11. URL: https://catalog-n.com/sovremennaya-ehlektronika-7-2022#sovremennaya-ehlektronika-7-2022-26
12. URL: https://catalog-n.com/sovremennaya-ehlektronika-8-2022#sovremennaya-ehlektronika-8-2022-26
13. URL: https://catalog-n.com/sovremennaya-ehlektronika-9-2022#sovremennaya-ehlektronika-9-2022-09
14. URL: https://www.xsoccorp.com/post/are-cryptographically-relevant-quantum-computers-prepared-to-disrupt-classical-encryption
15. URL: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html
16. URL: https://www.express.co.uk/news/science/841491/hacking-encryption-quantum-computer-physics
17. URL: https://www.cyber.gov.au/acsc/view-all-content/publications/post-quantum-cryptography
18. URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two
19. URL: https://homepages.cwi.nl/~rdewolf/qcnotes.pdf
20. URL: https://users.math-cs.spbu.ru/~okhotin/teaching/quantum_2020/migrin_ivanov_quantum_2020_shor.pdf
21. URL: https://quantum-computing.ibm.com
22. URL: https://arxiv.org/pdf/1111.4147.pdf
23. URL: https://arxiv.org/pdf/1903.00768.pdf
24. URL: https://iopscience.iop.org/article/10.1088/1367-2630/18/2/023023
25. URL: https://www.nature.com/articles/ncomms5213
26. URL: https://www.sciencedirect.com/science/article/pii/S0370157322003118
27. URL: https://www.techspot.com/news/96603-ibm-announces-osprey-quantum-processor-433-qubits.html
28. URL: https://www.nature.com/articles/s41534-021-00478-z
29. URL: https://arxiv.org/abs/1411.4028v1
30. URL: https://static-content.springer.com/esm/art%3A10.1038%2Fs41534-021-00478-z/MediaObjects/41534_2021_478_MOESM1_ESM.pdf
31. URL: https://arxiv.org/abs/1812.01041
32. URL: https://www.dwavesys.com/solutions-and-products/systems/
33. URL: https://journals.jps.jp/doi/abs/10.7566/JPSJ.88.061012
34. URL: https://arxiv.org/ftp/arxiv/papers/2106/2106.08681.pdf
35. URL: https://www.nature.com/articles/s41598-022-17867-9
36. URL: https://journals.aps.org/prb/abstract/10.1103/PhysRevB.80.052506
37. URL: https://link.springer.com/chapter/10.1007/978-4-431-66879-4_283
38. URL: https://www.nature.com/articles/s41598-022-17867-9#Sec12
39. URL: https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/
40. URL: https://www.forbes.com/sites/arthurherman/2021/12/09/booz-allen-sounds-the-alarm-on-chinas-coming-quantum-harvest/?sh=25c373e653e5
41. URL: https://www.xsoccorp.com/company
42. URL: https://techmonitor.ai/technology/emerging-technology/post-quantum-encryption-threat-already-here
43. URL: https://www.etsi.org/events/2117-2023-02-9th-etsi-iqc-quantum-safe-cryptography-workshop
44. URL: https://www.controlgap.com/blog/quantum-cryptography-for-risk-managers
45. URL: https://csrc.nist.gov/CSRC/media/Projects/stateful-hash-based-signatures/documents/stateful-HBS-misuse-resistance-public-comments-April2019.pdf
46. URL: https://link.springer.com/chapter/10.1007/978-3-030-25510-7_12
47. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6281621/
48. URL: https://dl.acm.org/doi/abs/10.1145/3402192
49. URL: https://openquantumsafe.org/about/
50. URL: https://arxiv.org/pdf/1903.02176.pdf
51. URL: https://www.ibm.com/cloud/blog/introducing-quantum-safe-crypto-tls-for-ibm-key-protect?mhsrc=ibmsearch_a&mhq=Quantum-Safe
52. URL: https://www.ibm.com/products/z16
53. URL: https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world
54. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
55. URL: https://pq-crystals.org/kyber/
56. URL: https://pq-crystals.org/dilithium/
57. URL: https://falcon-sign.info/
58. URL: https://sphincs.org/
59. URL: https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world
60. URL: https://openquantumsafe.org/about/
61. URL: https://openquantumsafe.org/applications/
62. URL: https://hub.docker.com/r/openquantumsafe/curl-dev