Квантовая криптографическая катастрофа. Часть 2

Виктор Алексеев (victor.alexeev@gmail.com)

Во второй части статьи рассматриваются современные квантовые процессоры и перспективы применения платформ на их основе для решения различных вычислительных задач. Отдельное внимание уделено обзору технологии постквантовой криптографии.

В начале ноября 2022 года концерн IBM анонсировал новую модульную платформу «System Two», способную объединять несколько квантовых процессоров в единую систему с универсальными интерфейсами между ними. Этот «строительный блок» предназначен для создания гибридных квантово-ориентированных сетей, которые позволят взаимодействовать классическим компьютерам с квантовыми суперкомпьютерами с помощью специального облачного решения.

Первым квантовым процессором в этом проекте стал IBM «Osprey», имеющий 433 рабочих кубита (рис. 1) [27].

Идея использования гибридного квантово-классического метода для факторизации больших чисел была реализована в 2021 году [28]. Авторы этой работы из «Zapata Computing» и «Massachusetts Institute of Technology», по существу, использовали для процесса факторизации метод VQE, назвав его «Variational Quantum Factoring – VQF». В этом методе VQF используется схема сведения задачи факторизации к модели с минимизацией гамильтониана и известного алгоритма Фархи (Quantum Approximate Optimization Algorithm) [29].

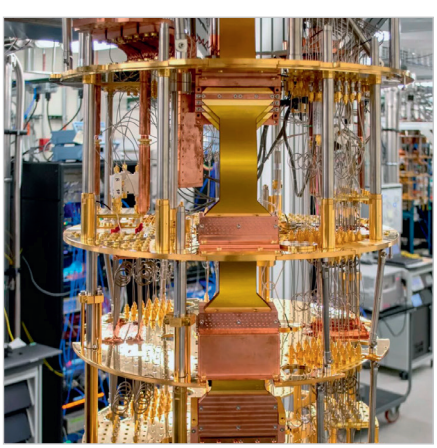

Рис. 1. Новый универсальный квантовый компьютер с вентильным управлением IBM «Osprey» имеет 433 кубита [27]

Алгоритм VQF позволяет адаптировать задачу факторизации к решению сложной задачи с помощью метода оптимизации. Приблизительно этот процесс можно представить себе следующим образом. Факторизация числа N, содержащего n бит, сводится в конечном итоге к нахождению двух простых множителей p и q, удовлетворяющих условию $N = pq$. Поскольку простые числа p и q могут быть представлены nq и np битами соответственно, то процесс факторизации можно рассматривать как задачу, обратную обычному двоичному умножению. Иными словами, если известно значение i-го бита результата факторизации Ni, то задача состоит в том, чтобы найти биты простых множителей $\{pi\}$ и $\{qi\}$.

Стандартная процедура двоичного умножения p и q позволяет создать систему уравнений, которым должны удовлетворять {pi} и {qi}, а также биты, соответствующие переносу из i-й в j-ю позицию.

С помощью этих уравнений можно привязать конкретные биты задачи факторизации к узлам задачи оптимизации. Подробно этот процесс сопоставления задачи факторизации и квантового алгоритма Изинга описан в работе [29]. Таким образом, решение задачи факторизации сводится к нахождению минимума гамильтониана с помощью квантового алгоритма модели Изинга. Корректировка требуемого количества кубитов, а также операции с анзацем осуществлялись с помощью стандартного цифрового компьютера. Квантовые вычисления проводились с использованием ресурсов европейского квантового центра «IBM Boeblingen». Подробно экспериментальная часть этой работы описана в документе [30].

Схема эксперимента «вариационной квантовой факторизации» показана на рис. 2.

В левой части рис. 2 проиллюстрирован выбор количества итерационных шагов и необходимых кубитов в зависимости от значения числа N, которое нужно разложить на множители. После этого определялся гамильтониан задачи.

Задача оптимизации и подготовка пробного состояния реализовывались на квантовом компьютере IBM с использованием многослойной методики QAOA (центральная часть рис. 2).

В правой части рис. 2 показана схема заключительной стадии классической обработки, объединяющей результаты измерений на квантовом устройстве с классической предварительной обработкой и оценки успешности алгоритма.

Описанный алгоритм VQF и методика анзаца QAOA были применены для факторизации трёх целых чисел: 1 099 551 473 989, 3127 и 6557. Количество кубитов, необходимых для каждого экземпляра, зависит от объёма выполняемой классической предварительной обработки. Для 1 099 551 473 989 было использовано 24 итерации классической предварительной обработки, 8 итераций для 3127 и 9 – для 6557.

При этом использовался послойный метод QAOA, подробно описанный в работе [31].

С одной стороны, рассмотренный метод VQF представляется полезным для факторизации составных чисел, поскольку результат вычислений квантового компьютера можно быстро проверить на классическом компьютере. С другой – в ходе экспериментов было обнаружено, что вероятность успешного нахождения сомножителей при факторизации выходит на некоторый уровень насыщения и далее перестаёт расти по мере увеличения количества итераций и количества используемых кубитов. Этот эффект связан с релаксацией и декогерентностью на более глубоких уровнях QAOA. Когерент-

Рис. 2. Схема эксперимента факторизации с использованием метода VQF [30]

ный шум может быстро возрастать с увеличением количества итераций, что существенно ограничивает на данном этапе развития квантовых технологий возможности метода VQF в плане увеличения диапазона факторизации.

Проблема когерентных шумов менее остро проявляется в адиабатических квантовых вычислителях (AQC), поскольку в этом случае не требуются логические кубиты для исправления ошибок. Принцип действия AQC принципиально отличается от универсального цифрового квантового компьютера с вентильной обработкой (UDGQC).

В компьютерах UDGQC вычисления контролируются с помощью унитарных квантовых логических вентилей, изменяющих состояние каждого кубита. В противоположность этому AQC не имеет вентилей и не использует алгоритмы и квантовые операторы. Принцип действия AQC заключается в том, что вся система в целом устанавливается в начальное положение с помощью внешнего магнитного поля и далее контролируется адиабатический процесс её перехода в основное состояние. На практике широкое распространение получил упрощённый вариант адиабатических квантовых вычислений, получивший название «quantum annealing processing solver QAP» (вычислитель с квантовым отжигом). В этом устройстве эволюционный процесс идёт «не сам по себе», а регулируется внешним магнитным полем [13]. В настоящее время направление QAP быстро развивается во всём мире, прежде всего благодаря разработкам и массовому производству канадской фирмы D-Wave. Последняя модель процессора для квантового отжига фирмы D-Wave имеет 5000 кубитов [32].

Идея использования квантового отжига для задач перебора данных типа факторизации не нова и активно обсуждается в последние годы.

Квантовый отжиг подразумевает нахождение минимального из возможных значений гамильтониана физического процесса, который описывается конкретной математической моделью. Практически это применимо к модели Изинга, описывающей в общем случае систему, состоящую из размещённых в узлах решётки спинов, которые могут принимать только два возможных конечных состояния: либо вверх, либо вниз. Поэтому большинство прикладных задач квантового отжига решалась с помощью преобразования алгоритма некоторой начальной задачи в алгоритм типа Изинга.

В рассмотренных выше примерах с использованием VQF и квантового вентильного компьютера для решения задач факторизации изначальный гамильтониан преобразовывался и сводился к модели Изинга. В случае квантового отжига в «классическом варианте D-Wave» это сделать крайне сложно из-за отсутствия универсального управления каждым кубитом с помощью квантовых вентилей, как это сделано в компьютерах типа UDGQC. Поэтому преобразованный гамильтониан далеко не полностью соответствовал изначальному гамильтониану решения задачи факторизации.

Для того чтобы разрешить это противоречие, авторы работы [33] предложили задействовать дополнительную встроенную в квантовый процессор схему умножителя двоичных чисел и контроллера логических величин с использованием булевой алгебры.

Эту идею развили и реализовали экспериментально японские учёные из «National Institute of Advanced Industrial Science and Technology» [34].

В своей публикации они продемонстрировали возможности применения квантового отжига для прямого решения задачи факторизации с использованием изначального гамильтониана с булевыми таблицами истинности. Был предложен вариант квантового отжига QAP с модернизированной схемой процессора и изменённой топологией расположения кубитов. Идея нововведений заключалась в том, что непосредственно в квантовый процессор QAP была встроена схема квантового умножителя с булевой логикой, позволявшая совершать операции умножения состояний кубитов, а также сравнивать результаты этих операций с помощью логических модулей. Таким образом, задавая кубитам различные состояния в соответствии с некоторой таблицей истинности, можно было перемножать двоичные числа. Следующий шаг заключался в том, чтобы определить минимальное значение разности между результатом умножения и числом N, подлежащим факторизации. То есть дальнейший процесс решения задачи факторизации проходил в соответствии со сценарием «классического» варианта квантового отжига, когда система сама переходит в основное состояние с минимумом гамильтониана.

Таким образом, стало возможным решать задачу разложения больших чисел с помощью процесса квантового отжига без предварительной трансформации на программном уровне первоначально заданного гамильтониана факторизации. Сам алгоритм квантового отжига при этом несколько усложнился и замедлился за счёт того, что на определённом этапе необходимо было задействовать квантовый процессор для выполнения промежуточных вычислений.

Подробное описание этого эксперимента и новые результаты измерений авторы опубликовали в августе 2022 года в журнале Nature [35].

На рис. 3 показана схема вычислительной ячейки экспериментальной установки для исследования факторизации с помощью квантового отжига, использованная в «Национальном

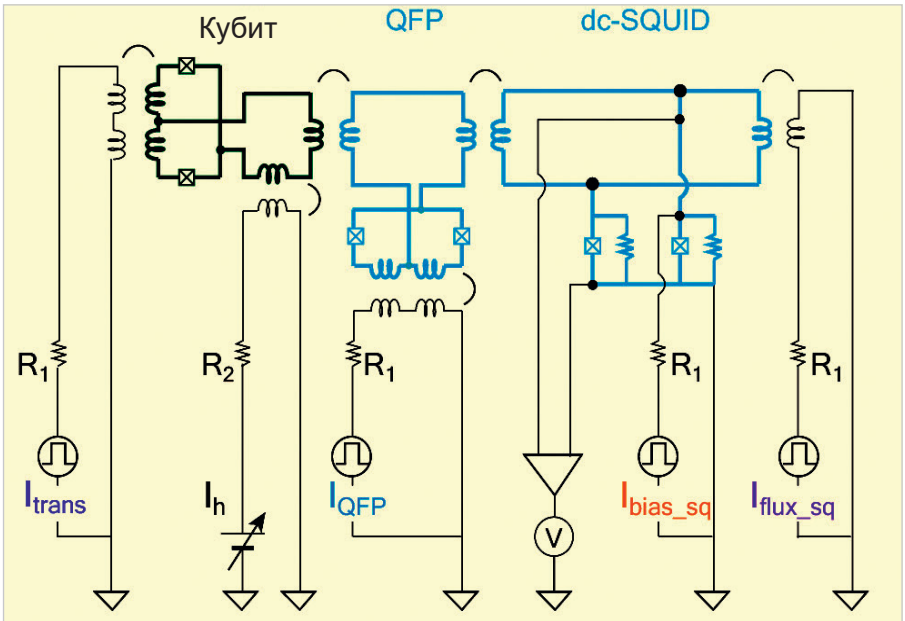

Рис. 3. Схема вычислительной ячейки экспериментальной установки для исследования факторизации с помощью квантового отжига, использованная в «Национальном институте передовых промышленных и научных технологий Японии» [35]

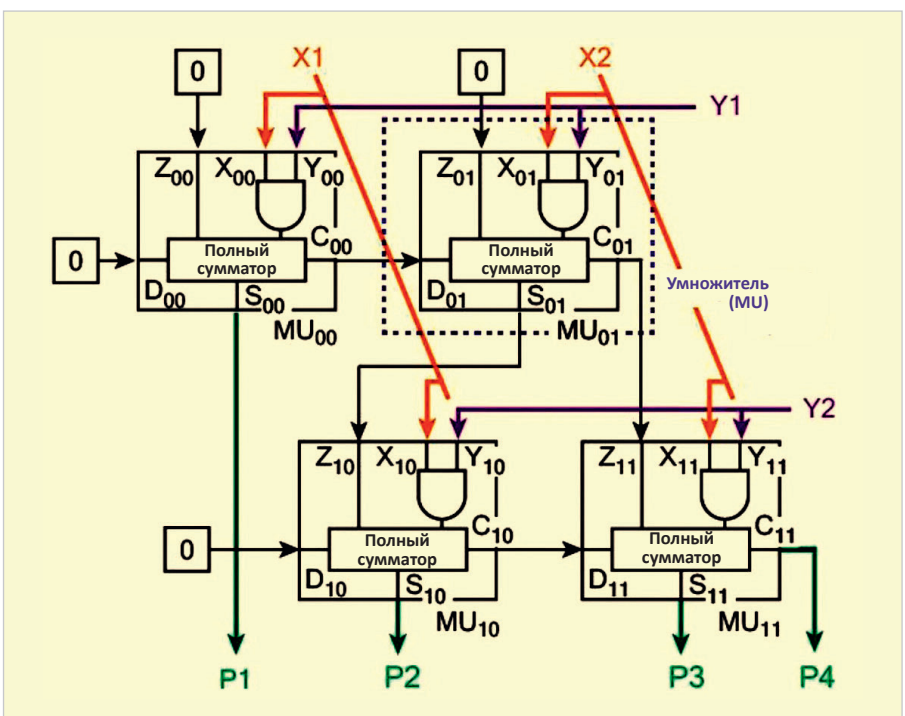

Рис. 4. Схема 4-битного логического квантового умножителя состояний кубитов [35]

институте передовых промышленных и научных технологий Японии».

В состав вычислительной ячейки входят: сверхпроводящий потоковый кубит с ДП, квантовый логический элемент (QFP) и устройство считывания (SQUID).

Кубиты в этой схеме изготовлены на одной подложке с системой считывания SQUID по технологии с четырьмя слоями Nb, допускающей плотность критического тока до 1 мкА/мкм^2 [36].

Конструктивно кубит состоит из большой сверхпроводящей петли, содержащей считыватель на основе dc-SQUID (dc superconducting quantum interference device) и вставленной в неё малой петли с джозефсоновскими переходами (ДП). Сверхпроводящий квантовый интерферометр SQUID имеет два состояния с постоянным током, текущим по часовой стрелке или против часовой стрелки, которые определяют ноль и единицу кубита.

Параметрон квантового потока (QFP – quantum flux parametron) представляет собой устройство реализации квантовой логики на основе сверхпроводящих джозефсоновских переходов [37].

Управление кубитами осуществляется с помощью следующих токов, меняющих состояния сверхпроводящих переходов: I_{trans} – ток поперечного поля; I_{QFP} – ток инжекции квантового параметрона; I_{bias_sq} – ток управления SQUID; I_{flux_sq} – ток модуляции SQUID; I_h – ток общего внешнего смещения в кубите. Эти токи можно изменять в соответствии с алгоритмом квантового отжига.

Схема 4-битного логического квантового умножителя (4-bit multiplier unit MU) приведена на рис. 4.

Умножитель состоит из четырёх MU, обозначенных на рис. 4 пунктирным прямоугольником.

Блок умножителя состоит из четырёх элементов MU_{ij} ($i=0–1, j=0–1$), каждый из которых обеспечивает определённую функцию:

- X_{ij} и Y_{ij} – общие входы (inputs);
- Z_{ij} – вход суммы (sum-in);
- D_{ij} – процессорный вход (carry-in);
- C_{ij} – процессорный выход (carry-out);
- S_{ij} – результат вычислений (summation).

Схемы, показанные на рис. 3 и 4, являются элементами процессора квантового отжига, размещённого в криогенной камере с температурой внутри 10 мК. Такая температура необходима для поддержания нормальной работы низкотемпературных сверхпроводящих кубитов. Работоспособность этого процессора была подтверждена многократными экспериментами, результаты которых сравнивались с точными модельными расчётами на стандартном компьютере с бинарной логикой.

Используя двоичное числовое представление, можно говорить о том, что на общие входы подаются массивы чисел потенциальных сомножителей факторизации ($P=M\times N$): $M=(X_{01}\,X_{00})_{(2)}$ и $N=(Y_{11}\,Y_{01})_{(2)}$ соответственно.

На выходе полного сумматора (full adder) будет результат двоичного перемножения: $P=(P_4\,P_3\,P_2\,P_1)_{(2)}=(C_{11}\,S_{11}\,S_{10}\,S_{00})_{(2)}$.

Вход D01 может быть зафиксирован на 0, независимо от X1 и Y1.

Гамильтониан такой системы можно записать в виде

$$H=\sum_i h_i\sigma_z^{(i)}+\sum_{i>j}J_{ij}\sigma_z^{(i)}\sigma_z^{(j)}.$$

В этой формуле: $\sigma_z^{(i)}$ – матрица Паули, действующая на кубит i; J_{hi} – константа, характеризующая смещение кубита i; J_{ij} – константа связи между кубитами i и j. В общем случае h_i и J_{ij} являются безразмерными программируемыми входными параметрами, которые перебираются в процессе квантового отжига. С помощью перечисленных выше токов задаются необходимые параметры, обеспечивающие каждую итерацию.

Ток поперечного магнитного поля и ток внешнего смещения вызывают инжекцию квантов магнитного поля в кубите. Параметрон QFP обнаруживает этот магнитный всплеск, усиливает его и транслирует на интерферометр dc-SQUID. При этом SQUID вырабатывает сигнал, который уже может быть измерен обычной аналоговой электроникой.

Состояние кубита определяется каждые 0,6 мкс и обычно оценивается в течение 104 итераций. В результате определяются все возможные комбинации токов, соответствующие искомым множителям.

Безразмерные коэффициенты, соответствующие локальным токам смещения h_i и попарным связям J_{ij}, для процессора с шестью кубитами могут принимать следующие значения:

$h_1 : h_2 : h_3 : h_4 : h_5 : h_6 : J_{12} : J_{13} : J_{14} : J_{15} : J_{16} : J_{23} : J_{24} : J_{25} : J_{26} : J_{34} : J_{35} : J_{36} : J_{45} : J_{46} : J_{56} = 1 : -1 : -2 : -2 : +4 : +2 : +1 : +2 : +2 : -4 : -2 : +2 : +2 : -4 : -2 : +4 : -8 : -4 : -8 : -4 : +8$,

где h_i и J_{ij} определяются с помощью выражения

$$h_1 = M_i \cdot I_{hi} \cdot I_{qi};$$
$$J_{ij} = M_{ij} \cdot I_{qi} \cdot I_{qj}.$$

В реальных терминах физического эксперимента значения M_i, h_i и J_{ij} определяются следующим:

- M_i – взаимная индуктивность между кубитом i и локальной линией смещения;
- I_{hi} – ток, протекающий через локальную линию смещения;
- I_{qi} – постоянный ток в кубите i;
- M_{ij} – взаимная индуктивность между кубитами i и j соответственно.

Измеряя эти величины и следуя алгоритму квантового отжига, можно с помощью описанного квантового процессора реализовать прямой процесс факторизации с использованием вычислителя с квантовым отжигом.

Полное подробное описание работы рассмотренной схемы факторизации приведено в [38].

Следует также отметить возможную схему будущих проектов, предложенную авторами [34]. Одно из возможных направлений, которое найдёт применение в ближайшем будущем, заключается в том, что вместо создания единого мощного квантового компьютера, способного решать любые задачи, имеет смысл развивать универсальные открытые гибридные квантовые сети, объединяющие компьютеры с бинарной логикой и квантовые вычислители, ориентированные на решение конкретных задач (рис. 5).

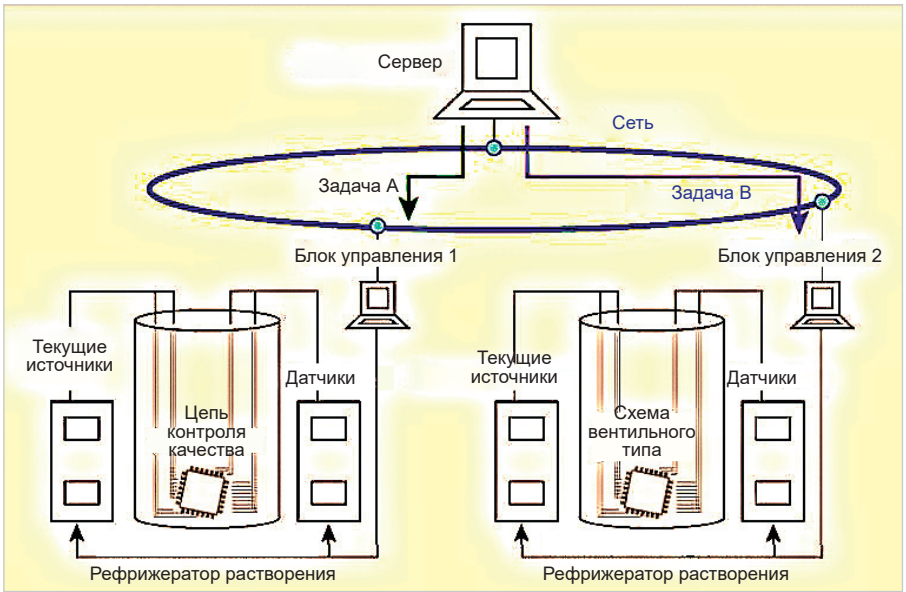

Рис. 5. Один из вариантов универсальных открытых гибридных квантовых сетей, объединяющих компьютеры с бинарной логикой и квантовые вычислители, ориентированные на решение конкретных задач [34]

Следует сказать, что, несмотря на значительные технологические и научные инновационные решения, которые были получены ведущими мировыми фирмами и университетами за 20 лет, прошедших с момента первой демонстрации квантовой факторизации, на сегодняшний день не существует квантового компьютера, который может решать задачи разложения сложных чисел лучше, чем компьютеры с бинарной логикой.

Постквантовая криптография

Потребовалось примерно десять лет интенсивных научных поисков после публикации результатов первых экспериментов по квантовой факторизации, чтобы понять, что «лобовая атака» с попыткой решить проблему путём увеличения количества кубитов в принципе не может увенчаться успехом на том уровне науки и технологий, которым человечество обладает на сегодняшний день. Поскольку ажиотаж, связанный с разработкой CRQC, постепенно утих, многочисленные лаборатории, образовавшиеся в результате «шифровального бума», переключились на новые направления. Одни лаборатории продолжили развивать технологии квантовых вычислений и переключились на направления, связанные с моделированием задач квантовой химии и физики. Другие фирмы отказались от первоначально заявленной цели (универсальный цифровой квантовый компьютер с вентильным управлением) и начали искать другие применения кубитов [13].

Третьи фирмы предпочли заниматься специфическим направлением, получившим название «постквантовая криптография» (post-quantum cryptography PQC), целью которого стала разработка квантово-безопасной криптографической технологии, устойчивой к квантовым атакам [39].

Наибольшее распространение практически во всех областях получили шифры с открытым ключом, такие как, например, RSA и ECC. В принципе, подобные шифры с ключами небольших размеров возможно взломать с использованием современных вычислительных мощностей и известных математических методов, таких как целочисленная факторизация, дискретное логарифмирование, метод эллиптической кривой. Однако большие ключи пока ещё разложить за «разумное» время не представляется возможным.

Тем не менее эксперты считают, что серьёзная опасность, существующая

Рис. 6. «XSOC CORP» предлагает надёжную защиту от уязвимости Apache Log4j [41]

сегодня, заключается в том, что спецслужбы разных стран стараются собирать максимальное количество зашифрованной информации в надежде на то, что её будет можно расшифровать в будущем при проявлении соответствующих технологий [40].

Поэтому целесообразно пытаться максимально обезопасить закрытую информацию уже сегодня, используя новейшие разработки. Один из лидеров в этой области – фирма «XSOC CORP» – предлагает различные варианты расширяемых криптосистем «Quantum-Safe» и симметричные транспортные ключи шифрования. Основное преимущество продукции этой фирмы заключается в том, что модернизация устаревших систем реализуется без необходимости их замены при полном сохранении защищаемых данных. В качестве примера можно привести надёжную защиту, которую «XSOC CORP» предлагает от уязвимости Apache Log4j, ставшей причиной серии массовых атак на веб-серверы по всему миру на протяжении декабря 2021 года (рис. 6) [41].

Основная задача «постквантовой криптографии» заключается в создании коммерчески доступных квантово-устойчивых алгоритмов с открытым ключом, предназначенных для широкого пользования [42].

В Европе это направление развивается в проекте «Quantum Safe Cryptography» под эгидой ETSI (Европейский Институт Стандартов и Телекоммуникаций) [43].

В США проблемы криптобезопасности курирует Национальный институт стандартов и технологий США (NIST). Эта организация в настоящее время занимается разработкой и утверждением стандартов постквантовой криптографии. С этой целью в 2016 году NIST объявил открытый конкурс на новый «постквантовый» стандарт шифрования. В первом туре этого конкурса, который завершился в 2017 году, приняло участие 69 фирм и университетов из разных стран мира.

В настоящее время развиваются два наиболее общих направления постквантовой криптографии. Одно из этих направлений связано с модернизацией старых систем и адаптации новых разработок в существующие системы безопасности. Для реальных разработок рекомендуется использовать симметричные алгоритмы при условии больших размеров ключей. В этом плане можно отметить криптографические алгоритмы с удвоенным размером ключа и различного рода хэш-функциями [44]. Основная тенденция этих разработок связана как с переходом ко всё более длинным симметричным ключам, так и с увеличением самой длины ключей RSA. Например, при обычном использовании AES-128 необходимо 3072 бита для эквивалентной надёжности ключей RSA. Протокол AES-256 требует уже ключ RSA длиной 15 КБ. В рамках изучения возможностей применения хэш-функций для систем PQC перспективным представляется специальное оборудование, включающее хэш-сигнатуру с сохранением состояния для встроенного ПО (stateful hash signatures for firmware) [45].

В качестве ещё одного примера можно привести работы по модернизации ключей «KEMS – key encapsulation mechanisms», позволяющие адаптировать классические алгоритмы для квантовых вычислителей. Например, немецкие математики из университета «Technische Universität Darmstad» работают с моделями гибридных протоколов обмена ключами с проверкой подлинности. Для точного определения различных квантовых сценариев вводится понятие безопасности для самих ключевых механизмов инкапсуляции (KEMS). Кроме того, предлагается метод построения гибридных KEMS для обмена ключами в TLS 1.3 [46].

Второе направление непосредственно связано с квантовыми технологиями. В первую очередь в этом классе следует отметить работы по генерации и распределению квантовых ключей. Основная идея здесь заключается в использовании квантовых компьютеров для генерации случайных ключей. Метод «Quantum Key Distribution – QKD» предназначен для создания и распределения симметричных криптографических ключей между двумя отдельными пользователями. Такой подход обеспечивает безопасность удалённого согласования ключей, которое невозможно перехватить без обнаружения пользователями. В этой области много оригинальных новых идей. Так, в работе [47] предложено независимое от измеряющего устройства квантовое распределение ключей (measurement device independent quantum key disctribution – MDI-QKD). Эффективность метода была подтверждена лабораторными и полевыми испытаниями.

Подробный анализ сетей QKD, протоколов маршрутизации, сигнализации и методов моделирования приведён в обзоре [48].

Интерес представляют также варианты защиты с использованием квантовых состояний, нейтрализующие друг друга. Принцип этого метода заключается в том, чтобы создать средства, затрудняющие сам процесс квантовых вычислений, вызывая необходимость отменять результаты манипуляций и делать бесконечные повторные расчёты [49].

В качестве меры противодействия CRQC рассматриваются и такие нетрадиционные схемы, как, например, шифр Вернама с передачей ключей с помощью запутанных фотонов, распределение фотонных ключей (Photon Key Distribution – PKD) и другие методы симметричного шифрования [50].

Учитывая важность проблемы, исследованиям по направлению post-quantum cryptography (PQC) уделяют внимание ведущие разработчики систем квантовых вычислений. Так, концерн IBM анонсировал новый пакет криптографических приложений IBM Quantum-Safe, предназначенный для защиты наиболее ценных данных клиентов в эпоху квантовых вычислений. Учитывая, что

среди клиентов IBM есть крупнейшие мировые банки и транснациональные корпорации, можно не сомневаться, что финансовая поддержка проекта будет весьма значительной [51].

Новая платформа IBM z16 обеспечивает устойчивость гибридных облачных платформ с помощью инновационных квантово-безопасных технологий [52].

Активное участие в разработках проектов PQC принимает концерн Google.

Одно из основных направлений исследований в этой области направлено на использование TLS и ALTS с гибридным методом обмена ключами для защиты внутреннего трафика. Совместно с Cloudflare в 2019 году был проведён эксперимент, в ходе которого были реализованы два сеанса постквантовых обменов ключами. Также была продемонстрирована возможность их интеграции в стек TLS Cloudflare с последующей реализацией на пограничных серверах и в клиентах Chrome Canary. В 2021 году Google провёл тестирование постквантовой конфиденциальности в TLS на расширенной сети [53].

В июле 2022 года завершился этап конкурса, объявленного в 2016 году, и NIST выбрал четыре алгоритма, которые будут финансироваться и разрабатываться для защиты данных от будущих атак с использованием квантового компьютера [54].

В категории общего шифрования (general encryption), которое предназначено для защиты информации, передаваемой в общедоступных сетях (public network), был выбран алгоритм CRYSTALS-Kyber, использующий сравнительно небольшие ключи шифрования, которыми две стороны могут легко обмениваться на высоких скоростях обмена данными [55].

Во второй категории задач, касающихся обеспечения безопасности цифровых подписей (digital signatures) и аутентификации личности (identity authentication), были выбраны три алгоритма: CRYSTALS-Dilithium [56], FALCON [57], SPHINCS+ [58].

Первые два из отмеченных в этой категории протоколов были выбраны из-за их эффективности. Протокол SPHINCS+ был выбран благодаря использованию инновационного математического аппарата.

Необходимо подчеркнуть, что в разработках SPHINCS+ принимали активное участие сотрудники Google [59].

Тема «постквантовой криптографии» крайне актуальна и обширна. Полноценный обзор этой темы выходит за рамки данной статьи. Однако стоит рекомендовать желающим испытать свои силы в данном направлении обратить внимание на проект «Open Quantum Safe – OQS», в котором может принять участие любая организация и любое физическое лицо [60].

Желающие начать экспериментировать с постквантовой криптографией могут использовать готовые образы «Docker», содержащие версии OpenSSL/curl, Apache httpd и nginx с поддержкой постквантов [61].

Для разработчиков также имеется возможность использовать готовые образы с возможностью расширения и установки кода [62].

Что касается появления на свет квантового компьютера CRQC, реально способного взламывать любые шифры и обрушать Интернет, то день его рождения, получивший международное название «Q-Day», никто точно не знает. Одни специалисты считают, что это может случиться уже через десять лет. Другие специалисты говорят, что на это может потребоваться больше 30 лет [42].

Несмотря на огромные технические проблемы, направление квантовых вычислителей интенсивно развивается. В предыдущих разделах этой статьи можно было увидеть как изменялась сама идея квантового релевантного компьютера (CRQC). Двадцать лет назад первоначальная схема CRQC предполагала использование универсального цифрового квантового компьютера с вентильной обработкой, типа IBM-Q. К началу зимы 2022 года мировое научное сообщество уже имело исчерпывающие доказательства возможности реализации процесса факторизации с помощью совершенно других устройств, таких как вариационный решатель с квантовым отжигом и решатель на базе квантового отжига со встроенным синтезатором гамильтониана факторинга. Что будет дальше, предположить сложно. Если, как считают некоторые специалисты, появятся гибридные облачные платформы, объединяющие мощные стандартные компьютеры и специализированные квантовые вычислители разного типа, то «Q-Day» может наступить раньше, чем его ожидают.

Поэтому общее мнение специалистов в области криптографии заключается в том, что поздно будет заниматься вопросами криптобезопасности, когда день «Q-Day» настанет. Разрабатывать противоядие нужно уже сейчас.

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. URL: 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. URL: 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. 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

НОВОСТИ МИРА

Первый вице-премьер пообещал представить в марте концепцию технологического развития России до 2030 года

Концепцию технологического развития РФ до 2030 года планируется утвердить в марте текущего года, сообщил первый заместитель председателя правительства Андрей Белоусов на совещании с экспертным сообществом и представителями профильных ведомств.

Документ готовится по поручению президента России по итогам состоявшегося в июле 2022 года заседания Совета по стратегическому развитию и национальным проектам.

Концепция определит понятие, цели, задачи и принципы достижения технологического суверенитета страны, а также целевые показатели технологического развития. Она состоит из трёх разделов: устойчивый технологический суверенитет, технологии как фактор роста экономики и развития социальной сферы и технологическое обеспечение устойчивого функционирования производственных систем – говорится на сайте правительства.

Каждый из этих разделов включает подготовку кадров и развитие компетенций, устранение регуляторных барьеров, создание условий для роста малых технологических компаний, локализацию производства, запуск крупных промышленных проектов и другие.

Речь идёт о смене ключевой модели взаимодействия двух процессов. Это развитие науки (когда основным продуктом является знание, а технологии скорее побочны) и развитие производства (когда технологии – обязательный составной элемент, подчинённый логике освоения рынков, повышения конкурентоспособности). Данные процессы расположены рядом, попытки выстроить между ними взаимосвязь уже предпринимались, но результаты недостаточны, отметил Андрей Белоусов.

В обсуждении концепции приняли участие представители бизнес-сообщества (венчурных фондов, институтов развития, крупнейших банков), научно-образовательных кругов (РАН, ведущих вузов и научных организаций) и органов власти (министерства, администрация президента, представители крупнейших регионов).

industry-hunter.com

НОВОСТИ МИРА

Нидерланды взбунтовались против США из-за запрета литографов для Китая

Нидерланды решили больше не ограничивать поставки литографического оборудования для выпуска чипов в Китай, руководствуясь указаниями американских властей. Теперь консультироваться по этому поводу правительство страны будет с государствами-партнёрами в Европе и Азии.

Нидерланды не будут ограничивать поставки литографического оборудования в Китай для производства полупроводников «по указке» США, об этом заявила глава Минторга Нидерландов Лизе Шрайнемахер (Liesje Schreinemacher), пишет издание South China Morning Post.

Чиновница объяснила решение тем, что экспортные ограничения в отношении Поднебесной, которые американские власти приняли в октябре 2022 г., серьёзно «поменяли правила игры», так как включают в себя запрет поставок сканеров диапазона DUV (193 нм).

Теперь окончательный вердикт выносить будут лишь после обсуждения ситуации с представителями европейских и азиатских государств. Решающее слово останется за властями Франции и Германии. Причина в том, что ASML Holding NV – крупнейший в Голландии и в мире вендор литографического оборудования, используемого в производстве микросхем, – владеет долей в немецкой компании Carl Zeiss и использует её оптику для сканеров. Консультироваться будут также с коллегами из Японии и Тайваня, промышленность которых играет большую роль в мировой индустрии полупроводников.

Шрайнемахер признала, что у США есть повод опасаться чрезмерной зависимости от Азии, где производится 80% передовых чипов, которые потенциально могут использовать в военно-промышленном комплексе. Чиновница уточнила, что если все стороны будут согласны ввести беспрецедентный мораторий на поставки в Поднебесную продукции для производства чипов, его введут.

Последние несколько лет власти США пытаются нанести сокрушительный удар по крупнейшим китайским производителям микроэлектроники, чтобы затормозить развитие КНР в этом направлении. Среди них – компании Semiconductor Manufacturing International Corp. (SMIC) и Hua Hong Semiconductor Ltd.

С 2019 г. Нидерланды под давлением администрации Дональда Трампа (Donald Trump) запрещали компании ASML поставлять китайцам ту продукцию, на которую указывали США. В основном речь шла о литографических сканерах диапазона EUV (13,5 нм), которые нужны для выпуска чипов по самым актуальным нормам на самых современных технологических процессах.

При этом запрет не касался поставок сканеров диапазона DUV (193 нм) последнего поколения – «железа», которое используется в производственных линиях для выпуска чипов по более старым техпроцессам. DUV-установки на поколение отстают от передовых (EUV), однако DUV-литография – всё ещё самый распространённый метод изготовления микросхем для автомобилей, телефонов, компьютеров и робототехники.

Используя эту лазейку, ASML лишь в 2021 г. продала в Китай оборудования на сумму около 2,1 млрд евро – это соответствует 16% общих продаж.

В октябре 2022 г. администрация Джо Байдена (Joe Biden) запретила компании продавать в Китай сканеры диапазона DUV. После этого компания велела своим американским сотрудникам прекратить обслуживание, доставку или оказание поддержки всем клиентам в Поднебесной до дальнейшего уведомления.

КНР для ASML была третьим по величине рынком сбыта после Тайваня и Южной Кореи, где её приобретали TSMC, SK Hynix и Samsung. Ещё летом 2022 г. на фоне слухов о новых ограничениях акции компании обвалились на 7,2% всего за один день. Представители компании отмечали, что мораторий на поставки обернётся большими убытками, так как поставками занимаются и компании-посредники.

Олег Изумрудов, исполнительный директор консорциума отечественных разработчиков систем хранения данных «РосСХД», заметил, что США, введя мораторий, по сути, потребовали от ASML самоубийства.

«У нидерландской компании законтрактовано, то есть предоплачено, оборудования на 7-8 лет вперёд, а сервисной поддержки – на сотни миллиардов евро, – уточнил эксперт. – При невыполнении контрактных обязательств сумма штрафов может достигнуть рекордного уровня в триллион евро. Это фактически убьёт и весь бизнес ASML, и в целом обрушит бизнес всех заказчиков ASML и Philips/NXP».

Пока санкции не приводят к прямому самоубийству компаний, а по сути – стран, для которых это основа налоговых поступлений в их бюджет, уточнил эксперт, они будут получать поддержку правительств других государств.

От сотрудничества с YMTC, крупным китайским вендором флеш-памяти, в октябре 2022 г. также были вынуждены отказаться американские Applied Materials, KLA и Lam Research. Теперь, чтобы продавать в Поднебесную новое и поддерживать существующее оборудование, они должны запрашивать лицензию на экспорт технологий у Бюро промышленности и безопасности (BIS) Министерства торговли США.

Если ASML поставляла компании сканеры, то американские компании – инструменты для метрологии, травления, осаждения, контроля и сортировки штампов. При этом пока у Китая остаются поставщики оборудования для производства полупроводников в Японии.

russianelectronics.ru

«Видеонаблюдать» за россиянами станут по миллионам импортозамещающих IP-камер

Массовое производство IP-камер видеонаблюдения и их внедрение начнётся в России к концу 2023 года.

Об этом пишут «Известия» со ссылкой на дорожную карту «Новое индустриальное программное обеспечение», утверждённую правительством в декабре 2022 года.

По данным издания, за реализацию проекта отвечает Минцифры. Серийный выпуск IP-камер должен быть налажен в 2023–2024 годах, а также выстроены каналы их сбыта. За этот же период заказчикам должно быть поставлено не менее одного миллиона таких устройств. В следующем году планируется наладить производство и поставки камер с улучшенными характеристиками, а именно: с изменяемым фокусным расстоянием объектива.

В качестве соорганизаторов проекта и заказчиков камер в документе указаны «Ростелеком» и «ЭР-Телеком Холдинг», предоставляющие клиентам услуги видеонаблюдения. В пресс-службе «Ростелекома» изданию пояснили, что компании являются якорными заказчиками в рамках проекта и призваны обеспечить спрос. Параметры проектов находятся на стадии согласования, и говорить о деталях пока преждевременно, подчеркнул представитель компании.

В пресс-службе Минцифры сообщили изданию, что производством камер займётся ООО «Электра». Операторы связи планируют устанавливать камеры на улицах по заказу городских властей, а также на государственных и частных территориях, если у владельца есть такой запрос.

Ранее сообщалось, что курение сигарет и вейпов в неположенных местах в России начнут отслеживать с помощью камер видеонаблюдения. В настоящее время начинается разработка прототипа системы, позволяющей оперативно отловить нарушителя и подать сигнал в соответствующие органы или ответственным за безопасность.

russianelectronics.ru