Физик Николас Пулидо стоит у прототипа квантового компьютера в Брунсвике, Германия.

Квантовая вычислительная техника

ВОЗМОЖНОСТИ И ОПАСНОСТИ

Квантовые компьютеры способны взломать криптографию, лежащую в основе финансовой стабильности

Жозе Деодору, Михаил Горбанёв, Маджид Малайка и Тахсин Саади Седик

В Древней Греции воины отправляли секретные депеши, обернув полоску пергамента вокруг древка и написав на нем. Послания их могли быть расшифрованы только человеком с древком такого же диаметра. Это один из самых ранних примеров криптографии. Современные тайны, такие как интернет-коммуникации, цифровые банковские услуги и электронная торговля, защищены от посторонних глаз мощными компьютерными алгоритмами. Однако вскоре эти до сих пор неприступные криптографические коды могут остаться в прошлом.

Квантовые компьютеры могут достичь такого уровня оптимизации, который позволит взламывать многие современные шифровальные ключи за меньшее время, чем требуется для их генерации обычным цифровым компьютерам. Финансовым учреждениям следует незамедлительно защитить свои системы кибербезопасности на будущее. Если этого не сделать, под угрозой окажется финансовая стабильность.

Квантовая революция

Квантовые вычисления — это использование для выполнения вычислений квантовых явлений, таких как *суперпозиция* и *запутанность*. Основной единицей квантового компьютера является квантовый бит (сокращенно — *кубит*). Обычно она реализуется через квантовые свойства субатомных частиц, такие как спин электронов или поляризация фотона. В то время как каждый двоичный бит, используемый в современных цифровых компьютерах, представляет собой величину, составляющую либо ноль, либо единицу, кубиты представляют собой одновременно и ноль, и единицу (или их сочетание). Это явление называется суперпозицией. Квантовая запутанность — это особая связь между парами или группами квантовых эле-

Квантовые компьютеры способны значительно превзойти по производительности цифровые компьютеры, работающие по законам классической физики.

ментов. Изменение состояния одного элемента влияет на другие запутанные элементы мгновенно — независимо от расстояния между ними.

Увеличение числа кубитов обеспечивает экспоненциальный рост скорости выполнения вычислений. Чтобы сравняться с мощностью одного кубита, требуется два традиционных двоичных бита; для соответствия по мощности двум кубитам требуется четыре бита; для соответствия трем кубитам требуется восемь битов; и так далее. Для моделирования квантового компьютера со всего лишь 54 кубитами потребуется примерно 18 квадриллионов битов традиционной памяти. Чтобы достичь мощности квантового компьютера из 100 кубитов, потребовалось бы больше битов, чем есть атомов на всей нашей планете. А для компьютера из 280 кубитов потребуется больше битов, чем имеется атомов в известной нам Вселенной.

Квантовые компьютеры способны значительно превзойти по производительности цифровые компьютеры, работающие по законам классической физики. Уильям Филлипс, лауреат Нобелевской премии по физике, сравнил скачок от сегодняшней технологии к квантовой с переходом от счетной доски к цифровому компьютеру. До недавнего времени это так называемое *квантовое преимущество* или квантовое *«превосходство»* было не более чем теорией. Однако в 2019 году компания Google воспользовалась квантовым компьютером для выполнения определенной вычислительной задачи всего за 200 секунд. По словам представителей компании, для решения этой задачи самому мощному на тот момент цифровому суперкомпьютеру потребовалось бы 10 000 лет.

Возможности

Сложные вычислительные задачи похожи на поиск выхода из лабиринта. Традиционный компьютер попытается найти его, последовательно пройдя по всем путям, пока не достигнет выхода. В отличие от этого суперпозиция позволяет квантовому компьютеру попробовать все пути одновременно. Это кардинально сокращает время поиска решения.

Решая задачи с большей точностью и скоростью, чем цифровые компьютеры, квантовые компьютеры способны ускорить процесс научных открытий и инноваций, произвести революцию в моделировании и имитационных расчетах работы финансовых рынков, а также расширить возможности машинного обучения и искусственного интеллекта. Их можно использовать для моделирования субатомных частиц, молекулярных взаимодействий и химических реакций. Это может произвести революцию в области химической технологии и материаловедении и позволить создать новые материалы, например, твердотельные батареи. Квантовые компьютеры также могут помочь нам понять процессы изменения климата.

Квантовые компьютеры могут преобразовать и финансовую систему. Они могут выполнять более точное моделирование методом Монте-Карло, используемое для прогнозирования поведения рынков с помощью имитационных моделей ценообразования и рисков, практически в режиме реального времени. Не будет необходимости упрощать эти модели нереалистичными допущениями. Квантовые компьютеры также могли бы решать задачи оптимизации — такие как распределение капитала, определение портфельных инвестиций или управление наличностью в банкоматных сетях — за малую толику того времени, которое требуется цифровым компьютерам. Квантовые компьютеры также могут ускорить настройку алгоритмов машинного обучения. Время, нужное для этого цифровым компьютерам, увеличивается экспоненциально с каждым добавляемым измерением. С квантовыми компьютерами дело обстоит иначе.

И опасности

При этом существуют и риски. Вычислительная мощь этих могучих квантовых машин может угрожать современной криптографии. Это чревато далеко идущими последствиями для финансовой стабильности и конфиденциальности. Современная криптография основана на трех основных типах алгоритмов: *симметричные ключи, асимметричные ключи* (также известные как *открытые ключи*) и *функции хеширования*. При использовании симметричных ключей для шифрования и расшифровки сообщения используется один и тот же ключ. В асимметричной криптографии используется пара связанных ключей (один закрытый, другой — открытый). Сообщение, зашифрованное одним ключом, может быть расшифровано только парным ключом. Эти алгоритмы широко используются для цифровой аутентификации, цифровых подписей и защиты данных. Функции хеширования преобразуют цифровые входные данные в уникальный набор байтов фиксированного размера. Они используются для безопасного хранения паролей и поддержки цифровых профилей.

Эти криптографические алгоритмы в основном успешно справляются с задачей защиты данных. Даже наиболее современные цифровые суперкомпьютеры и методы криптоанализа не позволяют взламывать их достаточно быстро. Однако квантовые компьютеры смогут решать сложные математические задачи во много раз быстрее, чем цифровые суперкомпьютеры.

ФОТО: GETTY IMAGES / PICTURE ALLIANCE / JULIAN STRATENSCHULTE

Финансовые учреждения должны незамедлительно предпринять шаги по подготовке к переходу на новые криптографические системы.

Это сделает асимметричную криптографию устаревшей и ослабит другие криптографические ключи и хэши. Теоретически, полностью функционирующий квантовый компьютер может взломать асимметричный ключ за несколько минут. Особенно уязвимы открытые ключи, поскольку большинство из них основаны на задаче факторизации: цифровым компьютерам трудно найти два простых числа, отталкиваясь от их произведения. Квантовые компьютеры, напротив, могут делать это без особых усилий.

Асимметричные ключи широко используются для защиты коммуникаций через Интернет. Успешные атаки на эти алгоритмы поставят под угрозу соединения, используемые в финансовой системе, включая мобильный банкинг, электронную коммерцию, платежные операции, снятие наличных денег в банкоматах, коммуникации через виртуальные частные сети и т.д. и т.п. К уязвимым приложениям, в которых используется криптография с открытым ключом, также относятся популярные цифровые активы, такие как Bitcoin и Ethereum, а также защищенные паролем веб-приложения. Самый известный из этих протоколов, HTTPS, используется на 97 из 100 ведущих вебсайтов мира.

Для некоторых приложений уже может быть слишком поздно что-то менять. Любая информация, которая сегодня считается безопасной, может быть перехвачена и сохранена, чтобы быть расшифрованной позже, когда будут созданы достаточно мощные квантовые компьютеры. Фактически, почти любое зашифрованное личное или финансовое сообщение, отправленное и сохраненное сегодня, может быть расшифровано задним числом с помощью мощного квантового компьютера. Большинство финансовых учреждений и регулирующих органов пока не осознало этих новых видов рисков.

Наперегонки с машиной

Гонка по разработке новых стандартов и алгоритмов квантово-безопасного шифрования уже началась. В США Национальный институт стандартов и технологии проводит конкурс на разработку квантово-безопасных алгоритмов шифрования. В институте надеются объявить победителя к 2024 году. Европейский институт по стандартизации в области электросвязи также среди лидеров в этой области. Эти усилия способствуют деятельности других органов, устанавливающих стандарты. Однако из-за ретроспективных рисков у финансовых учреждений остается лишь ограниченное время для внедрения новых стандартов.

Финансовые учреждения должны незамедлительно предпринять шаги по подготовке к переходу на новые криптографические системы. Им следует начать с оценки ретроспективных и будущих рисков, связанных с квантовым компьютерами, в том числе из-за информации, которая, возможно, уже была перехвачена и может быть использована спустя годы. Затем финансовым учреждениям следует разработать планы по переводу текущей криптографии на квантово-устойчивые алгоритмы. Это включает в себя проведение инвентаризации криптографии с открытыми ключами, которую они используют сами, а также криптографии, используемой сторонними поставщиками. Уязвимые алгоритмы необходимо будет перевести на постквантовую криптографию. Финансовым учреждениям также следует развивать криптографическую гибкость, чтобы можно было плавно обновлять алгоритмы. Хотя мероприятия по замене алгоритмов гораздо проще, чем переход к пост-квантовым стандартам, опыт показывает, что они могут быть чрезвычайно дезорганизующими. На их осуществление часто уходят годы или десятилетия.

МВФ предстоит сыграть важную роль в повышении осведомленности своих стран-членов о рисках для финансовой стабильности, связанных с квантовыми компьютерами, и в содействии распространению квантово-безопасных стандартов и практик. Фонду следует поощрять страны-члены к тесному сотрудничеству в деле разработки стандартов квантово-безопасного шифрования для обеспечения межоперационной совместимости и принятия планов миграции шифрования для своих финансовых секторов.

Современные квантовые компьютеры очень чувствительны. Любое возмущение окружающей среды, например тепло, свет или вибрация, выводит кубиты из их квантового состояния и превращает их в обычные биты. Это приводит к ошибкам в расчетах. Тем не менее, не за горами машины, способные проводить вычисления с меньшим количеством ошибок и взламывать коды. Финансовым учреждениям следует осознать риски и защитить свои системы, пока не стало слишком поздно. В конце концов, история изобилует поучительными примерами того, как якобы нераскрываемые коды взламывались благодаря новой технологии. ФР

ЖОЗЕ ДЕОДОРУ — владелец платформы для сбора данных, **МИХАИЛ ГОРБАНЕВ** — старший экономист Департамента МВФ по вопросам стратегии, политики и анализа, **МАДЖИД МАЛАЙКА** — ведущий эксперт по цифровой трансформации и рискам кибербезопасности в Департаменте информационных технологий МВФ. **ТАХСИН САДИ СЕДИК** — заместитель начальника отдела Департамента стран Азиатско-Тихоокеанского региона МВФ.

Данная статья основана на Рабочем документе МВФ 21/71 «Квантовые вычисления и финансовая система: страшноватая динамика на расстоянии?»