Министерство науки и высшего образования

Российской Федерации

Федеральное Государственное

Автономное Образовательное Учреждение

Высшего Образования

Национальный ядерный университет «МИФИ»

Кафедра: «Финансовый мониторинг»

Постквантовое шифрование

Студент Монастырский М. О.

Группа С21-703

Москва 2024г.

Оглавление

[Что такое квантовый компьютер 2](#_Toc167045231)

[Квантовые компьютеры в жизни 2](#_Toc167045232)

[Квантовые компьютеры (пока) не угроза 3](#_Toc167045233)

[Квантовая угроза 4](#_Toc167045234)

[Постквантовое шифрование 4](#_Toc167045235)

[Пора применять 5](#_Toc167045236)

[Финальный штрих 6](#_Toc167045237)

# Что такое квантовый компьютер

Основное отличие квантовых компьютеров от традиционных, транзисторных, которыми все мы пользуемся сейчас, — то, как они работают с данными. Привычные нам устройства, от смартфонов и ноутбуков до суперкомпьютера-шахматиста Deep Blue, хранят все в битах — так называется мельчайшая единица информации, которая может принимать всего два значения: либо ноль, либо единица.

Бит можно сравнить с лампочкой, которая либо включена (единица), либо выключена (ноль). Файл, лежащий на диске, для компьютера выглядит как набор лампочек, из которых одни горят, а другие — нет. Если взять очень много таких лампочек, то, включив одни и выключив другие, можно собрать хоть фразу «тут был Альберт», хоть Мону Лизу.

Но когда устройство решает какую-то задачу, оно включает и выключает лампочки, постоянно записывая и стирая результаты промежуточных вычислений, чтобы они не забивали память. Это занимает время, так что если задача очень сложная, компьютер будет думать долго.

Квантовые компьютеры, в отличие от своих старших братьев, хранят и обрабатывают данные с помощью квантовых битов — кубитов. Последние могут не только «включаться» и «выключаться», но и находиться в переходном состоянии или даже быть включенными и выключенными одновременно. Продолжая аналогию с лампочками: кубит — это как светильник, который вы выключили, а он все равно продолжает моргать. Или кот Шредингера, который одновременно и жив, и мертв.

Поскольку лампочки в квантовом компьютере одновременно горят и не горят, это сильно экономит время. Поэтому он решает сложные задачи намного быстрее даже очень мощного классического устройства. Например, в Google утверждают, что их квантовая машина Sycamore за три с небольшим минуты провела вычисления, над которыми обычный суперкомпьютер в теории бился бы 10 000 лет! Вот это и называют серьезным термином «квантовое превосходство».

# Квантовые компьютеры в жизни

Итак, квантовые компьютеры очень быстро решают очень сложные задачи. Но почему они тогда просто не вытеснили медленные классические системы? Дело в том, что эта технология еще молода, а состояние «моргающей лампочки» — очень нестабильное, и чем больше в системе кубитов, тем труднее его поддерживать. А доступность сложных вычислений зависит в том числе от количества кубитов: с помощью двух лампочек, пусть и очень крутых, Мону Лизу не нарисуешь.

Есть и другие проблемы, мешающие квантовым компьютерам полностью заменить предшественников. Вы помните, что они обрабатывают информацию принципиально иначе? Это значит, что и программы для них нужны совершенно другие. На квантовый компьютер нельзя просто взять и установить Windows — надо с нуля разрабатывать специальную квантовую ОС и специальные же квантовые приложения.

И хотя такие попытки уже предпринимают ученые и IT-гиганты, пока что квантовые компьютеры работают примерно как внешние жесткие диски — подключаются к обычным компьютерам и управляются через них. И используются они для решения узкого круга задач — например, для моделирования атома водорода или поиска по базам данных. А вот выйти в Интернет или посмотреть видео с котиками с помощью квантового компьютера не получится.

Тем не менее многие считают квантовые вычисления перспективными. Первая компания, продающая бизнесу квантовые компьютеры, появилась еще в 1999 году. Сейчас в это направление вкладываются крупные организации, такие как американские Google, Honeywell и IBM (последняя уже предлагает клиентам доступ к своему квантовому компьютеру через облако), японская Toshiba и китайские Alibaba и Baidu. В 2019 году квантовыми технологиями заинтересовались и российские власти.

Правда, тут стоит оговориться: задача, которую решили в Google, не имеет никакой практической пользы, кроме демонстрации возможностей квантовых технологий. Погружаться в ее суть мы не будем, потому что это действительно сложно и не очень нужно обычному пользователю. Но если вы очень хотите убедиться в этом лично, описание задачи есть в отчете Google.

А еще не все согласны с утверждением Google про 10 000 лет. В IBM, например, уверены, что суперкомпьютер сможет решить эту же задачу пусть и не за три минуты, но всего за два с лишним дня. Хотя это, в общем-то, тоже ощутимая разница.

# Квантовые компьютеры (пока) не угроза

Как видите, квантовые компьютеры до сих пор — скорее игрушка для ученых, чем потребительские устройства или инструмент взломщика. Что, конечно, не значит, что в будущем они не станут ближе к жизни (и опаснее). Впрочем, эксперты в области защиты данных уже сейчас готовят на них управу. Но об этом — в следующий раз.

# Квантовая угроза

Между тем возможность взломать асимметричный шифр существует: алгоритм, способный справиться с этой задачей, еще в 1994 году разработал ученый Питер Шор. Реализовать этот алгоритм позволяет квантовый компьютер. В отличие от обычных устройств, работающих на основе полупроводниковых технологий, мощность квантовых растет экспоненциально. Поэтому их возможности значительно превосходят любые инструменты, которые сегодня используют хакеры.

Современные квантовые компьютеры пока не обладают мощностью достаточной для взлома систем на основе асимметричного шифрования. Но с начала 2000-х такие технологические гиганты, как IBM, Google, Intel ведут разработки по развитию квантовых вычислений, что приближает нас к кибератакам нового типа. По мнению большинства экспертов, первые случаи подобных атак могут быть зафиксированы до 2030 года. Впрочем, аналитики McKinsey предостерегают, что финансовый и государственный секторы, а также страховая индустрия могут столкнуться с ними уже в ближайшие два года.

Это подводит нас к понятию квантовой угрозы — риска, что злоумышленники могут уже сегодня сохранять конфиденциальные данные, зашифрованные асимметричной криптографией, чтобы дешифровать их в будущем при первой появившейся возможности. Неважно каким образом хакеры получат доступ к квантовым устройствам — будет ли это социальный инжиниринг, облачная платформа квантовых вычислений или трудоустройство в компанию-разработчика квантовых компьютеров. Важно лишь то, что все накопленные данные, актуальные на тот момент, будут расшифрованы и приведут к колоссальным потерям. Поэтому защищать их необходимо уже сегодня.

К таким данным с длинным жизненным циклом относятся в том числе персональные данные клиентов банков и других финансовых организаций, медицинских учреждений и мобильных операторов, а также информация, представляющая коммерческую и государственную тайны.

# Постквантовое шифрование

В ответ на квантовую угрозу специалисты по информационной безопасности стали разрабатывать новые методы защиты. Самым оптимальным по стоимости и скорости интеграции стали решения на основе постквантовых алгоритмов. Такие алгоритмы строятся на сложных математических задачах, при решении которых квантовые компьютеры не получают вычислительного преимущества. Стойкость постквантового шифрования гарантируется математическими доказательствами секретности каждого из алгоритмов — все они проверяются мировым научным математическим сообществом.

В частности, это алгоритмы, основанные на линейных кодах, теории решеток и хеш-функциях. Первый тип (code-based) основан на гипотезе, что декодировать случайный линейный код очень сложно. Первый алгоритм такого типа появился еще в 1978 году — это была система McEliece, одна из первых систем с открытым ключом. В тот момент об атаках с использованием квантового компьютера не было и речи, однако после появления алгоритма Шора, способного легко взломать используемое повсеместно шифрование, криптографы-исследователи вновь заинтересовались алгоритмом McEliece.

Другой тип схем постквантовой криптографии — алгоритмы на основе теории решеток. Такие схемы хорошо изучены и легко применимы на практике, в частности, их использует IBM в своих приложениях безопасности.

В постквантовом шифровании применяется и один из самых популярных криптографических инструментов — хеш-функция. Хеширование — это преобразование произвольного объема данных в уникальный набор символов фиксированной длины, расшифровать который очень сложно. А постквантовые алгоритмы с использованием хеш-функции делают декодирование сообщения невозможным, во всяком случае, всеми известными методами. Хеш-функция может лежать в основе электронной подписи, в частности, эта модель сейчас прорабатывается в России.

# Пора применять

Над интеграцией и пилотированием криптографических алгоритмов в свои продукты уже работают такие гиганты рынка, как Microsoft, Google, Verizon, Thales, Toshiba, Amazon, Cloudflare.

Так, весной 2022 года IBM представила новое поколение мейнфреймов (универсальных высокопроизводительных серверов) z16, которые используют для защиты данных постквантовую криптографию. z16 оснащен ускорителем на базе искусственного интеллекта, что позволяет быстро обрабатывать огромные объемы информации. Это критично, в частности, для финансовых компаний и медицинских организаций, то есть тех, чьи данные обладают долгим циклом жизни. Именно поэтому для их защиты IBM применяет продукты в области постквантового шифрования, построенные на теории решеток.

В то же время южнокорейский мобильный оператор LG Uplus (принадлежит LG Group) выпустил коммерческий сервис для проводной и беспроводной связи, устойчивый к атакам с помощью квантового компьютера. А уже осенью LG Electronics объявила, что будет использовать этот метод защиты для ряда задач, в том числе в технологии V2X (vehicle to everything) — обмена данными между автомобилями и объектами дорожной инфраструктуры.

В октябре 2022 года компания Cloudflare объявила о запуске поддержки постквантовой криптографии для всех веб-сайтов и API, обслуживаемых через ее сеть. По сути это делает доступным квантовое шифрование для 19% мировых веб-ресурсов. Это наглядно демонстрирует, насколько критично к квантовой угрозе относится одна из крупнейших сетевых инфраструктур.

В России работа по пилотированию постквантовых продуктов также идет полным ходом: в июне 2022 года отечественные специалисты подтвердили совместимость постквантового шифрования с российскими процессорами Baikal-M, в октябре — с процессорами «Эльбрус». Первой в стране финансовой организацией, пилотировавшей постквантовые алгоритмы, стал Газпромбанк — в 2022 году он обеспечил квантово-устойчивую защиту host-to-host соединения при проведении финансовых поручений.

# Финальный штрих

На сегодняшний день постквантовая криптография находится на стадии стандартизации. В США этот процесс курирует Национальный институт стандартов и технологий (NIST). На конкурсной основе эксперты выбирают наиболее квантово-устойчивые алгоритмы, которые лягут в основу стандартов постквантового шифрования. В 2022 году институт выбрал четыре алгоритма — они станут частью постквантового криптографического стандарта, окончательная доработка которого ожидается примерно через два года. В то же время Белый дом обязал госструктуры уже к маю 2023 года совершить всецелую подготовку к переходу на постквантовые алгоритмы.

В России разработкой стандартов постквантовых алгоритмов занялись в 2019 году под руководством Технического комитета 26, куда входят представители государственных и коммерческих организаций. Ожидается, что отечественные стандарты будут утверждены к 2024–2025 году. Рынок вступил в фазу активного формирования, а значит уже в ближайшие один-два года число пилотных проектов мирового уровня вырастет в разы.