Как криптография помогает раскрыть суть квантового преимущества

Дата публикации: 25.07.2025

Квантовые вычисления на протяжении последних лет стали синонимом технологического прорыва: они обещают радикально ускорить решение задач, неподъёмных даже для самых мощных суперкомпьютеров. Но возникает важный вопрос: в каких случаях квантовые компьютеры действительно превосходят классические, и почему это происходит не всегда? Исследование, проведённое учёными Киотского университета, предлагает удивительный и фундаментально новый ответ, объединив квантовую информатику с криптографией — двумя науками, обычно считающимися самостоятельными.

В основе исследования лежит понятие квантового преимущества — способности квантовой машины выполнять вычисления, невозможные или практически недостижимые для классических систем. До сих пор научное сообщество предлагало лишь частичные условия, объясняющие, при каких обстоятельствах квантовые алгоритмы побеждают. Новое исследование впервые определяет точные критерии этого явления, используя язык криптографической безопасности.

Учёные сосредоточились на доказательствах квантовости, в которых классический наблюдатель взаимодействует с квантовым устройством, чтобы убедиться в его реальной вычислительной силе. Оказалось, что возможность такого доказательства напрямую зависит от наличия так называемых односторонних криптографических задач — задач, которые легко решить в одну сторону, но почти невозможно — в обратную. Если такие задачи существуют в квантовой форме, то квантовое преимущество становится возможным. А если они не выполняются, то сама безопасность многих криптографических алгоритмов, в том числе традиционных и постквантовых, оказывается под угрозой.

В этом состоит прорыв: доказано, что квантовое преимущество и криптографическая безопасность — неразрывно связанные понятия. Если первое нарушается, рушится второе. Это открывает новый уровень взаимосвязи между вычислительной сложностью и защищённостью информации.

Эта работа имеет практические и теоретические последствия. С одной стороны, она создаёт фундамент для более надёжных тестов квантовых вычислений, которые станут основой будущих демонстраций квантового преимущества в лабораторных и прикладных условиях. С другой — углубляет наше понимание природы вычислений в квантовой физике и может быть шагом к построению новой классификации задач, в которых квантовая обработка действительно даёт ощутимый выигрыш.

Исследование Киотского университета демонстрирует, что квантовые вычисления и криптография — это не просто параллельные линии развития технологий, а глубоко взаимосвязанные научные области. Такое соединение открывает путь к новым теоретическим моделям и практическим достижениям, формируя фундамент для вычислительной эпохи будущего.

Ссылка: «Криптографическая характеристика квантового преимущества» DOI: 10.1145/3717823.3718133.