Квантовый случай как гарантия доверия: как физики превратили запутанность в источник идеальной случайности

Дата публикации: 27.06.2025

В мире, где данные становятся новой валютой, а цифровая безопасность — критически важным элементом инфраструктуры, надежность случайных чисел приобретает фундаментальное значение. Большинство компьютерных систем — от шифрования и блокчейнов до статистического моделирования и честных выборов — полагаются на генераторы случайных чисел. Однако традиционные алгоритмы, даже самые сложные, могут быть предсказуемыми или подверженными вмешательству. Ответ на этот вызов современности дала фундаментальная физика: ученые впервые в истории запустили публичный генератор случайных чисел, основанный не на программном коде, а на самой природе квантовой реальности.

Исследователи из Национального института стандартов и технологий (NIST) и Университета Колорадо в Боулдере создали CURBy — уникальный радиомаяк случайности, который ежедневно транслирует поток доказуемо случайных битов, сгенерированных на основе квантовой запутанности. Это не просто очередной генератор: его работа базируется на эксперименте Белла — ключевом тесте в квантовой механике, который демонстрирует, что запутанные частицы ведут себя с непредсказуемостью, не поддающейся классическим объяснениям. Сами Эйнштейн, Подольский и Розен когда-то ставили под сомнение, действительно ли природа случайна, но современные эксперименты опровергли их сомнения.

В установке CURBy используются пары запутанных фотонов, свойства которых коррелированы, несмотря на физическую удалённость. Когда один из фотонов измеряется, его результат полностью случаен, но корреляция между результатами обоих фотонов нарушает пределы, установленные классической физикой, что и делает возможным статистически обоснованное подтверждение истинной случайности.

Такая случайность, в отличие от алгоритмической, не может быть предсказана ни хакером, ни суперкомпьютером, ни гипотетическим демоном Лапласа. Это делает CURBy ценнейшим ресурсом для тех сфер, где особенно важно исключить влияние сторон и обеспечить максимальную прозрачность: выбор присяжных, лотереи, выборочные проверки, голосования, а также криптография, где важно, чтобы ключи не могли быть воспроизведены никаким способом.

Важно и то, что CURBy — это не только физический эксперимент, но и продвинутая система цифровой верификации. Сервис защищён Twine — собственной разработкой на основе децентрализованных журналов, аналогичных блокчейну, где каждый бит случайности фиксируется, отслеживается и может быть независимо проверен. Такой подход гарантирует защиту от манипуляций, а также повышает доверие к источнику, особенно в общественно значимых процедурах.

CURBy — это первый в мире публичный генератор случайных чисел, использующий квантовую нелокальность как первоисточник. Его уникальность в том, что каждый опубликованный бит сопровождается статистической гарантией непредсказуемости, подтвержденной законами квантовой механики. Иными словами, если «Бог действительно играет в кости», как теперь признают физики, то CURBy позволяет использовать эти броски кубика для пользы общества.

Качество и происхождение каждой случайной последовательности могут быть сертифицированы, чего не могут обеспечить традиционные генераторы. Это делает CURBy новым стандартом для приложений, в которых случайность является не просто требованием, а критерием справедливости и безопасности.

В ближайшем будущем такие квантовые маяки могут стать частью цифровой инфраструктуры: от национальных лотерей до децентрализованных финансовых систем, от распределенных вычислений до глобальной идентификации и защиты данных. CURBy символизирует переход от недоказуемой имитации случайности к подлинной, физически подтверждаемой случайности, которая, возможно, станет основой доверия в цифровом мире.

Ссылка: «Сильный тест локального реализма без лазеек» DOI: 10.1103/PhysRevLett.115.250402.