Фотонные чипы и квантовая магия: QRNG теперь можно встроить в любой гаджет.

Случайные числа стали краеугольным камнем информационных и коммуникационных технологий. Генераторы случайных чисел, алгоритмы или устройства, способные производить непредсказуемые числовые последовательности, сегодня обеспечивают безопасность связи между разными гаджетами, формируют статистические выборки и используются во множестве разнообразных приложений.

Исследователи из Toshiba Corporation — это японская многоотраслевая компания, которая занимается разработкой и производством различных продуктов и услуг. Она активна в таких областях, как электроника, энергетика, медицинская техника, информационные системы и другие. Toshiba известна своими инновационными технологиями и продуктами, такими как ноутбуки, телевизоры, полупроводниковые компоненты и многое другое. Компания играет важную роль на мировом рынке и вносит значительный вклад в развитие различных отраслей." data-html="true" data-original-title="Toshiba" >Toshiba Europe Ltd. разработали новый квантовый генератор случайных чисел (QRNG) на основе фотонной интегральной схемы, которую можно напрямую встраивать в гаджеты и компьютеры. Технология работает с впечатляющей скоростью — 2 Гбит/с.

«Случайность стала ценным ресурсом, поскольку она лежит в основе практически всех цифровых протоколов, обеспечивающих конфиденциальность связи», — поясняет Рэймонд Смит, старший научный сотрудник и соавтор исследования. Он указывает на потенциальные риски для безопасности, связанные с использованием псевдослучайных генераторов чисел (PRNG), которые являются всего лишь детерминированными алгоритмами и не могут выдавать полностью произвольные результаты.

Последние исследования доказали, что с помощью QRNG, использующих квантовые эффекты в природе, можно получать действительно непредсказуемые числовые последовательности. Смит и его коллеги из Toshiba экспериментировали именно с такими методами.

«Предыдущие исследования и идеи, вдохновившие нашу работу, были связаны со стремлением упростить аппаратную часть QRNG», — рассказывает Смит. «Обычно в QRNG применяются фотонные компоненты вроде лазеров и детекторов, которые громоздки и требуют особого обращения при интеграции с электроникой. Из-за этой сложности QRNG неудобны для массового производства и обходятся дорого. Однако интегрированная фотоника помогает преодолеть эти трудности».

Фотонные интегральные схемы (ФИС) позволяют ученым сконденсировать все ключевые оптические компоненты на один крошечный чип размером всего в несколько миллиметров. Кроме того, благодаря компактности технологии, ФИС можно использовать для измерения оптической интенсивности, необходимой для генерации случайных чисел.

«В последние годы Toshiba добилась ряда значительных достижений в области ФИС, включая разработку первой в мире системы квантового распределения ключей (QKD) на базе чипа», — говорит Смит. «Эта система включала в себя ФИС QRNG в 14-контактном корпусе типа «бабочка», оптический выход которого необходимо было соединить оптоволоконной линией с высокоскоростным фотодиодом на электронной плате».

«Основной целью недавнего исследования команды Toshiba была разработка полнофункционального QRNG на базе фотонно-интегральных схем, способного работать только с электрическими сигналами на входе и выходе. Кроме того, ученые планировали внедрить QRNG в реальные устройства для подтверждения его эффективности в действии».

«Обычно ФИС тестируются в контролируемых лабораторных условиях с использованием специализированного оборудования», — объясняет Смит. «Такой подход затрудняет оценку работы этой технологии после ее развертывания в реальных системах и различных эксплуатационных средах».

Смит и его коллеги разработали компактную печатную плату, в которую встроили созданный ими ФИС под названием «оптическое энтропийное ядро» (OEC). OEC имеет стандартный корпус, схожий с другими электронными чипами, размером 6 x 6 мм2. Плата, на которую он смонтирован, включает электронные модули, управляющие ФИС, а также модули для считывания генерируемых им хаотичных сигналов.

Так как же генерируется случайный сигнал? ФИС содержит два лазера, испускающих оптические импульсы со случайными фазами из-за квантовых шумов. Эти импульсы интерферируют друг с другом, порождая сигнал с непредсказуемой оптической интенсивностью, который затем преобразуется высокоскоростным детектором в случайный электрический импульс. Сигнал детектора обрабатывается платой и преобразуется в случайные биты, которые могут распространяться на сверхвысоких скоростях (Гбит/с).

Главным преимуществом нового QRNG на базе интегрированной фотоники является

низкая стоимость лежащей в его основе ФИС, а также возможность сборки на электронных платах с использованием стандартных серийных методов. Это может способствовать массовому развертыванию QRNG в различных электронных устройствах, сделав его доступной и высокопроизводительной альтернативой PRNG.

Для обеспечения безопасности окончательного выходного сигнала QRNG выполняет проверки работоспособности выхода OEC, подтверждая его корректное функционирование, и автоматически корректирует параметры управления OEC при необходимости.

Первоначальные испытания продемонстрировали, что OEC может работать так же надежно, как и другие стандартные электронные компоненты.

«Мы встроили плату QRNG в систему квантового распределения ключей (QKD) и непрерывно эксплуатировали ее в течение 38 дней, получая стабильный случайный сигнал, несмотря на значительные колебания температуры», — рассказывает Смит. «Этот тест демонстрирует готовность нашего QRNG к развертыванию в реальных системах и реальных условиях эксплуатации. Другим примечательным моментом является тот факт, что мы получили практически идентичные показатели производительности от всех восьми протестированных плат».