"СМАРТС-Квантелеком" разработал квантовый генератор случайных чисел

Рассказывает генеральный директор ООО "СМАРТС-Квантелеком" **А.Л.Алексеев**

DOI: 10.22184/2070-8963.2024.121.5.32.33

Компания "СМАРТС-Квантелеком", основанная в Санкт-Петербурге 10 лет назад докторами и кандидатами наук Университета ИТМО, сегодня стала одним из отечественных лидеров в областях квантовых коммуникаций и квантовой сенсорики. Решения компании применяются, в частности, в рамках Дорожной карты квантовых коммуникаций, которую успешно реализует ОАО "РЖД". В преддверии Международного военно-технического форума "АРМИЯ-2024" специалистами "СМАРТС-Квантелеком" разработано очередное инновационное устройство – физический квантовый генератор случайных чисел. О новой разработке и сегодняшнем дне компании корреспонденту "ПЕРВОЙ МИЛИ" рассказал генеральный директор ООО "СМАРТС-Квантелеком" А.Л.Алексеев.

Алексей Леонидович, какие достижения "СМАРТС-Квантелеком" за 10 лет существования стоит выделить особо?

За десятилетие мы прошли путь от стартапа, занимавшегося лабораторными исследованиями, до компании, разрабатывающей и производящей мелкосерийно оборудование промышленного уровня, которое сегодня используется, в том числе, на магистральной квантовой сети ОАО "РЖД". Большим достижением считаю также создание мощной научно-технической команды, одной из лучших в стране в нашей сфере. Это касается как разработчиков радиоэлектронной аппаратуры, так и научных сотрудников – без опоры на серьезные теоретические исследования успех в такой наукоемкой области как квантовые коммуникации сегодня невозможен.

Среди наших достижений в продукции отмечу выполненные в кратчайшие сроки для замены импорта разработку и налаживание выпуска интегрально-оптических СВЧ-модуляторов. А созданный нашими конструкторами детектор одиночных фотонов ни в чем не уступает продукции мирового лидера ID Quantique.

В продуктовом портфеле "СМАРТС-Квантелеком" появился физический квантовый генератор случайных чисел. Расскажите о новом устройстве.

Случайные числа являются необходимым ресурсом в большом числе как научных, так и практических приложений. Генераторы случайных чисел (ГСЧ) можно разделить на две категории: псевдослучайные и аппаратные (физические). Генерация псевдослучайных чисел основана на математических алгоритмах, позволяющих получать каждое последующее число путем преобразования предыдущего согласно заданному алгоритму. К сожалению, зная предыдущие числа и алгоритм, можно предсказать всю

последовательность, поэтому данное направление имеет изъяны с точки зрения информационной безопасности.

Известны два принципа реализации физических ГСЧ: на базе законов классической физики и на квантовой основе. В первых источником энтропии служит тот или иной процесс, описываемый законами классической физики, но, следовательно, детерминированность таких процессов оставляет злоумышленнику возможность воспроизвести генерируемые классическим ГСЧ последовательности.

При разработке ГСЧ мы поставили задачу обеспечить генерацию истинно случайных числовых последовательностей, что позволяет использовать устройство и для криптографических приложений, и выбрали в качестве физического источника энтропии квантовые процессы, которые по определению имеют вероятностную природу.

Такие генераторы могут быть основаны на разных квантовых эффектах. Обладая накопленной за годы экспертизой, наши разработчики пошли по пути создания решения, в котором источником энтропии являются флуктуации вакуума. Если сформулировать кратко, то вновь созданное устройство обеспечивает извлечение случайностей из квантового шума, который получается путем вычитания на балансном детекторе сигналов, полученных с выходов светоделителя. Итоговый сигнал при помощи обработки аналого-цифровым преобразователем превращается в истинно случайную последовательность.

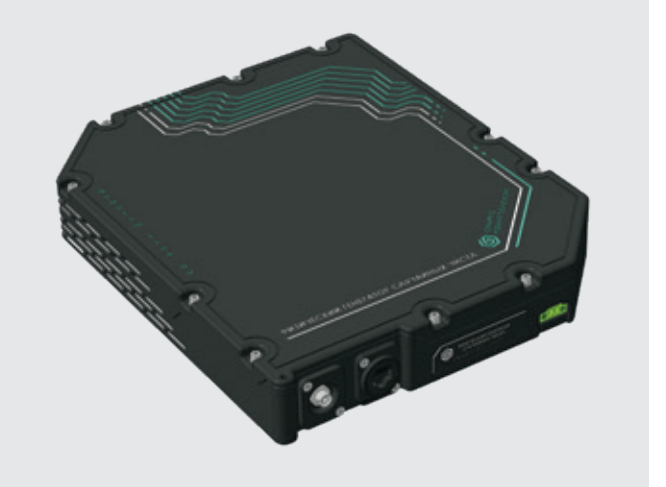
Это квантовое явление достаточно хорошо изучено учеными, имеется ряд инженерных воплощений таких устройств, но мы поставили перед собой задачу значительного их улучшения, в первую очередь с точки зрения миниатюризации и повышения скорости выработки случайных битовых последовательностей.

Где может использоваться новое устройство?

Последовательности случайных чисел необходимы в системах безопасности, криптографии (в том числе в квантовой криптографии), в научной сфере (статистике, моделировании различных систем и процессов). Потребность в ГСЧ должна особо возрасти в связи с приближением угрозы информационной безопасности со стороны квантовых компьютеров, поскольку такие генераторы существенно увеличивают длительность расшифровки. Мы считаем, что на горизонте нескольких лет генераторы истинно случайных чисел станут незаменимыми в криптографических системах, особенно в системах защиты информации государственной тайны.

В чем вы видите основные конкурентные отличия нового ГСЧ от представленных на рынке аналогов?

Наши конкурентные преимущества достигнуты за счет использования сложной математики и продвинутых



схемотехнических решений. Образец, который мы представляем на форуме "АРМИЯ-2024", обеспечивает скорость генерации случайных чисел порядка 500 Мбит/с. Это очень хороший показатель. Кроме того, нашим конструкторам удалось обеспечить малое энергопотребление и сделать устройство как можно более компактным. Последнее очень важно, так как ГСЧ планируется использовать в составе комплексов аппаратуры, где габариты весьма критичны.

В каких направлениях ведутся перспективные разработки ваших специалистов?

Продолжаются работы над совершенствованием ГСЧ. За счет создания аппаратной платформы с большим запасом мы планируем еще повысить скорость генерации случайных чисел. Мы активно работаем над созданием систем выработки и распределения квантовых ключей для абонентских подключений. Ведутся также разработки в сфере генерации квантовых ключей для связи по атмосферным оптическим каналам с мобильными объектами, например БПЛА, – такое решение крайне важно для масштабирования технологии квантовых коммуникаций на "последней миле". Все наши исследовательские задачи так или иначе направлены на создание систем квантовых коммуникаций нового поколения, с учетом понимания существующего опыта эксплуатации магистральных систем квантового распределения ключей и основных технологических факторов, ограничивающих масштабирование технологии здесь и сейчас.

Хочу пригласить всех интересующихся квантовыми коммуникациями на наш стенд № 1А2-1 на форуме "АРМИЯ-2024" в павильоне А.

Спасибо за беседу.

С А.Л.Алексеевым разговаривал С.А.Попов