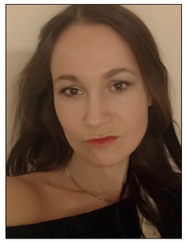

Елена ВЕРЕЩАГИНА
генеральный директор
ООО «СМАРТС-Кванттелеком»

ДРУГОЕ ШИФРОВАНИЕ

БЕСЕДЫ О КВАНТОВЫХ КОММУНИКАЦИЯХ[1]

Большинство найденных редакцией по «квантовой» теме статей числят ООО «СМАРТС-Кванттелеком» среди компаний, развивающих рынок «квантовых коммуникаций», причём помещают её когда в тройку лидеров, а когда и на первое место. Например: *«В России прототипы квантовых сетей с доверенными узлами построили только две организации: Университет ИТМО — совместно с КНИТУ-КАИ — в Казани, и с «Открытым кодом» — в Самаре, а также РКЦ — совместно с «Газпромбанком»*.

Тут стоит пояснить. Компания «СМАРТС-Кванттелеком» была учреждена в 2014 году выходцами из Университета ИТМО (Санкт-Петербург) и никогда не прекращала тесного сотрудничества с ИТМО в научной, внедренческой и образовательной сферах в области технологий квантовых коммуникаций вообще и квантового распределения ключей шифрования (КРК) в частности. Поэтому-то в ряде публикаций авторы и не вдаются в формальные детали кооперативных связей при осуществлении конкретных проектов.

По просьбе BIS Journal роль проводника по лабиринтам понятий, недомолвок и недоговорённостей сферы «квантовых коммуникаций» на этот раз любезно согласилась исполнить генеральный директор ООО «СМАРТС-Кванттелеком» Елена Верещагина. Скромность интервьюируемой нам удалось преодолеть вопросом: что же позволило компании стать одной из двух организаций, упомянутых в приведённой выше цитате? На который был получен следующий ответ:

«Работа «СМАРТС-Кванттелеком» корнями уходит в разработанный Университетом ИТМО подход кодирования квантовой информации в боковые частоты модулируемого излучения. Эффективность подхода показана в ряде работ, описывающих реализацию нескольких различных протоколов КРК. Здесь же следует отметить, что большая работа была проделана в части теоретического анализа секретности, суть которого была во введении только адекватных и чётких технических ограничений, в то время как описания многих современных протоколов КРК и систем, на них базирующихся, могут быть сформулированы достаточно нечётко (например, вышеупомянутый подход decoy state). Таким образом, конечная система КРК компании Кванттелеком может быть успешно использована в контексте квантовых сетей».

На наш взгляд, мы получили исчерпывающий ответ, который ещё больше повысил наше доверие к компании «СМАРТС-Кванттелеком» как партнёру, готовому открыто, не растекаясь мыслью по древу, раскрывать тайны своей профессии.

Уместно при этом отметить, что единственными «недостатками» приведённого ответа можно назвать употребление аббревиатуры КРК без её расшифровки и англицизм *«подход decoy state»*. Но аббревиатура КРК (квантовое распределение ключей [шифрования]) уже расшифровывалась в предыдущей публикации в первом номере BIS Journal, а понятие, кроющееся за нерусскими словами *decoy state*, как следует из стилистики ответа, уже обсуждалось на ранней стадии беседы.

После этой преамбулы нам остаётся только добавить, что одним из «крайних» дел «СМАРТС-Кванттелеком» на ниве квантовых коммуникаций стало участие в строительстве опытной магистральной квантовой сети вдоль железной дороги между Москвой и Санкт-Петербургом общей протяжённостью более 800 км. Проект разработан специалистами ОАО «РЖД» совместно с научными и производственными организациями страны, в нём заняты ведущие эксперты Университета ИТМО и компании «СМАРТС-Кванттелеком».

[1] Начало в BIS Journal № 1(40) / 2021, «Бизнес-ветвь потомков Ландавшица»

Модуль отправителя КРК

ВОПРОС-ОТВЕТ

BIS Journal. В открытой печати встретилось следующее утверждение: *«Фактически под термином «квантовая криптография» понимают метод конфиденциального квантового распределения криптографических ключей (КРК) (QKD — Quantum Key Distribution) между участниками сети, когда линия или сеть КРК решает задачу доверенного «курьера» по доставке секретных ключей абонентам…»* В связи с этим вопрос: технологии квантовых коммуникаций (ТКК) и квантовые технологии шифрования (КТШ) — это синонимы или КТШ — это часть ТКК? Квантовые технологии шифрования — это что? Только квантовое распределение ключей [шифрования], передача этих ключей по каналам связи? Или КТШ — это ещё и сами процедуры шифрования / дешифрования и передачи/приёма зашифрованных сообщений?

«СМАРТС-Кванттелеком». ТКК — представляют собой набор методов передачи квантовых состояний от отправителя к получателю. КРК — методы формирования ключей между сторонами, гарантия безопасности которых обеспечивается свойствами квантовых состояний. После процесса распределения ключей легитимные пользователи могут использовать классические технологии шифрования для закрытия конфиденциальной информации.

BIS Journal. В открытой печати встретилось утверждение о том, что *«…для поддерживающих технологий и в мире и в России отмечается максимальный, девятый, уровень TRL. Речь идёт об интеграции КРК с классическим шифратором, образовательных решениях, квантовом генераторе случайных чисел, классической постобработке квантовых ключей и детекторе одиночных фотонов»*. Что стоит за понятием уровня готовности технологий квантовых коммуникаций (TRL), измеряемых, вроде бы, отметками от 1 до 9? Девятка — это наличие коммерческого оборудования «на полках» или готовность документации для производства оборудования?

«СМАРТС-Кванттелеком». Есть документация, опытный образец, технология готова к производству.

BIS Journal. В открытой печати встретилось следующее утверждение: *«В большинстве магистральных оптоволоконных сетей применяется мультиплексирование по длине волны. Наличие классического сигнала в одной жиле оптоволокна создаёт засветки для квантового сигнала. Решением может быть как выделение тёмного волокна, так и мультиплексирование по времени, а также развитие методов оптической фильтрации для квантово-классического xWDM мультиплексирования. С этой точки зрения очень перспективным является КРК на непрерывных переменных». «Классический сигнал» — это синоним слов «оптический сигнал» и это не «квантовый сигнал»?* Какие простые аналогии можно было бы подобрать для подчёркивания различий между «классическим» и квантовым сигналами? Что такое КРК на «непрерывных переменных»?

«СМАРТС-Кванттелеком». Оба сигнала — и «классический» и «квантовый» — являются оптическими. Вся разница заключается в их интенсивности. У классического сигнала обычно

	ИТМО	Альфа	Браво
Скорость генерации просеянного ключа, бит/с	7200	2000	
Скорость генерации секретного ключа, бит/с	600	400	10
QBER,%	4,6%	5%	7–8%
Поддержка буфера для хранения ключей	Да	Да	Нет
Квантовый генератор случайных чисел	Нет	Нет	Да
Используемый протокол КРК	Фазовый на боковых частотах	BB84 decoy state	Собственная разработка
Детектор фотонов	Импортный	Собственная разработка	Собственная разработка
Поддержка стороннего СКЗИ	Да	Да	Нет

Таблица 1. Сравнение достижений, сделанных в стенах ИТМО, с достижениями конкурентов

высокая интенсивность (среднее число фотонов в импульсе/временном отрезке высокое), под квантовым излучением в данном контексте принято считать излучение по интенсивности близкое к однофотонному уровню энергии.

КРК на непрерывных переменных — отдельный класс протоколов, использующих на приемной стороне когерентное детектирование (гомодинное и гетеродинное детектирование) вместо детекторов одиночных фотонов. При таких методах приёма получатель имеет непрерывный сигнал на выходе приёмного модуля, который должен быть соответствующим образом обработан.

BIS Journal. Как вы можете прокомментировать следующую таблицу сравнения достижений, сделанных в стенах ИТМО, с достижениями конкурентов (таблица 1)?

Встретив такую таблицу, как вы прокомментируете разницу между «Фазовый на боковых частотах» и «Собственная разработка» в строке об используемом протоколе КРК? Как вы прокомментируете плюсы и минусы протоколов «Фазовый на боковых частотах» и BB84 decoy state? «СМАРТС-Квanttелеком» использует импортный детектор фотонов? Наличие собственных разработок детекторов фотонов — это хорошо или это может привести к удорожанию разработок по сравнению с использованием унифицированного детектора фотонов? Может ли вообще детектор фотонов быть унифицирован для разных ветвей развития оборудования КРК? Что такое QBER? QBER должно быть как можно меньше? Что мешает достичь идеала величины QBER?

«СМАРТС-Квanttелеком». QBER (Quantum Bit Error Rate) — характеризует величину ошибок в квантовом канале, соответственно, чем меньше это значение, тем выше дальность распределения ключа. Величина QBER не может быть полностью нулевой, в том числе из-за неидеальности. оптических и электронных компонентов системы КРК.

Комментировать что-либо под названием «собственная разработка» сложно, под этими словами может скрываться абсолютно всё что угодно, так что сравнение в данном случае выглядит не очень уместным. По поводу протоколов «Фазовый на боковых частотах» и BB84 decoy state можно сказать, что главное их различие заключается в разнице подходов к оценке наиболее опасных атак, из чего следуют все особенности их реализации.

На данный момент в ИТМО и «СМАРТС-Квanttелеком» разработан квантовый генератор случайных чисел. Разработка внедряется в существующую систему КРК.

В настоящее время «СМАРТС-Квanttелеком» использует детектор одиночных фотонов (ДОФ) собственной разработки. Разработка и производство собственных детекторов позволяет снизить стоимость комплекта КРК. Интерфейс ДОФ аналогичен интерфейсам импортных аналогов, имеющихся в продаже и использующихся в системах КРК.

Продолжение следует

ВМЕСТО ПРОМЕЖУТОЧНОГО ЭПИЛОГА

Одной из проблем «классической» сферы ИБ является неумение многих профессионалов ИБ разговаривать на понятном языке с пользователями и потребителями услуг защиты информации. Вместо такого, понятного, языка — англицизмы вкупе с «птичьим языком», где пара терминов может содержать смыслы, объяснение которых обычным языком требует целой страницы или очень точной яркой аналогии. В лице компании «СМАРТС-Квanttелеком» редакция нашла доброжелательного собеседника, готового последовательно разъяснять и помогать понимать нам скрытые смыслы публикаций в откровенно революционной сфере. Что позволит нам всем выйти в эту новую область с ясным пониманием и чётким видением.