КОД безопасности

QRATE QUANTUM SOLUTIONS

МТУСИ Московский технический университет связи и информатики

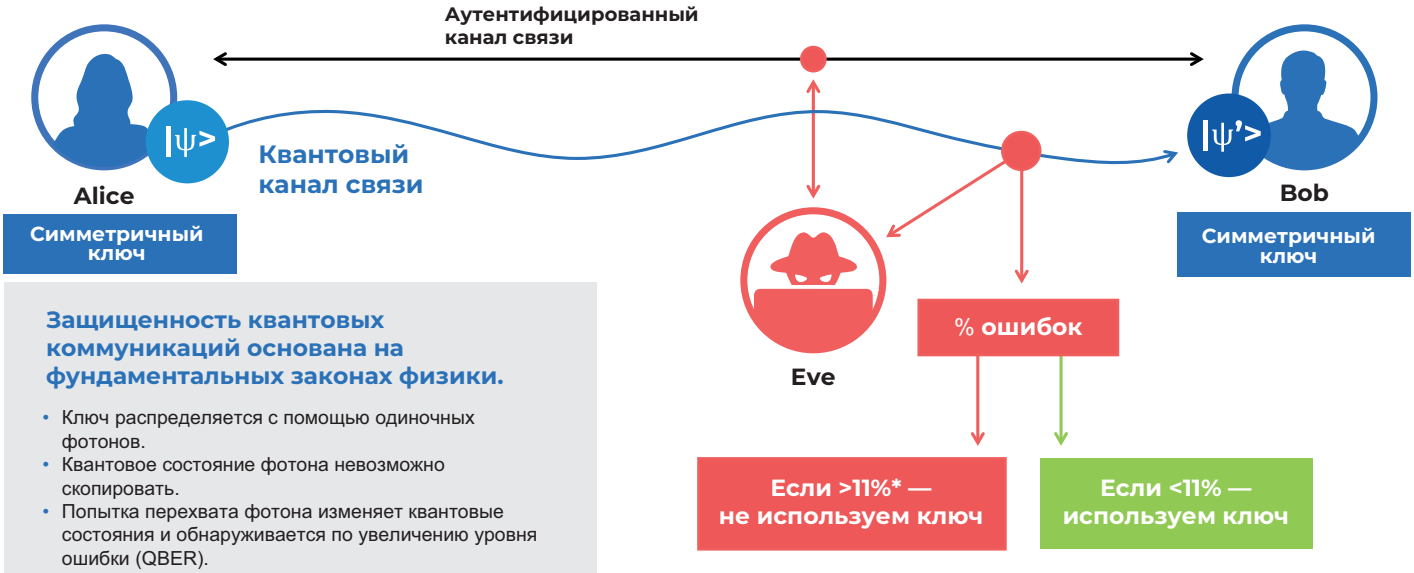
МИСиС Университет науки и технологий

Системы квантовых коммуникаций

Предпосылки создания

Квантовые вычислители, в частности квантовый компьютер, разрабатываемые компаниями Google, Baidu, IBM и др., благодаря квантовым эффектам способны решать многие математические задачи гораздо эффективнее классической полупроводниковой электроники. Среди таких математических задач особое место занимают задачи криптографии, на вычислительной сложности которых базируется повсеместно распространенное асимметричное и симметричное шифрование, технология блокчейн, протоколы распределения ключевой информации и иные. С появлением эффективного квантового вычислителя данные технологии оказываются под угрозой: асимметричное шифрование RSA и протокол распределения ключей Диффи-Хеллмана – квантовый алгоритм Шора, симметричное шифрование – квантовый алгоритм Гровера, блокчейн – атака 51%.
Непрекращающаяся цифровая трансформация бизнеса и промышленности порождает развитие индустриального Интернета вещей (IIoT). В этой связи увеличивается количество потенциальных целей для кибератак на объекты информационной инфраструктуры компаний и государственных организаций, за которыми стоят не только экономические, но и политические мотивы. С развитием информационной инфраструктуры увеличивается и объем передаваемой по каналам информации, а также усложняется коммутация. Технологии квантовых коммуникаций позволяют автоматизировать процесс распределения ключевой информации и обеспечить безопасное шифрование каналов любых топологий, исключая человеческий фактор, перебои в поставке ключей и гарантируя криптостойкость всех объектов компании.

Принцип работы



Защищенность квантовых коммуникаций основана на фундаментальных законах физики.

- Ключ распределяется с помощью одиночных фотонов.
- Квантовое состояние фотона невозможно скопировать.
- Попытка перехвата фотона изменяет квантовые состояния и обнаруживается по увеличению уровня ошибки (QBER).
- Если QBER не превышает заданного предела, то полученный ключ используется для шифрования.

* - Shor P.W., Preskill J. Simple proof of security of the BB84 quantum key distribution protocol // Phys. Rev. Lett. - 2000. - Vol. 85, 441.

Технология квантового распределения ключей (КРК) базируется на доказанной теореме о запрете клонирования произвольного неизвестного квантового состояния. Благодаря использованию этого принципа, технология квантовых коммуникаций решает широко известную проблему распределения симметричных ключей в сфере информационной безопасности, т.к. копирование одиночных фотонов, несущих в своем состоянии информацию о ключах, невозможно, а попытка перехвата будет обнаружена еще на стадии создания ключа до его использования. Этот эффект позволяет двум и более легитимным сторонам получить симметричный ключ, гарантированно известный только им.

Интеграция систем квантового распределения ключей при этом является простой и «мягкой», не требующей изменения устоявшейся инфраструктуры информационной безопасности компании. Устройство непрерывно генерирует ключ и по запросу передаёт на криптографическое оборудование, используя устоявшиеся протоколы ETSI и ПЛИВ.

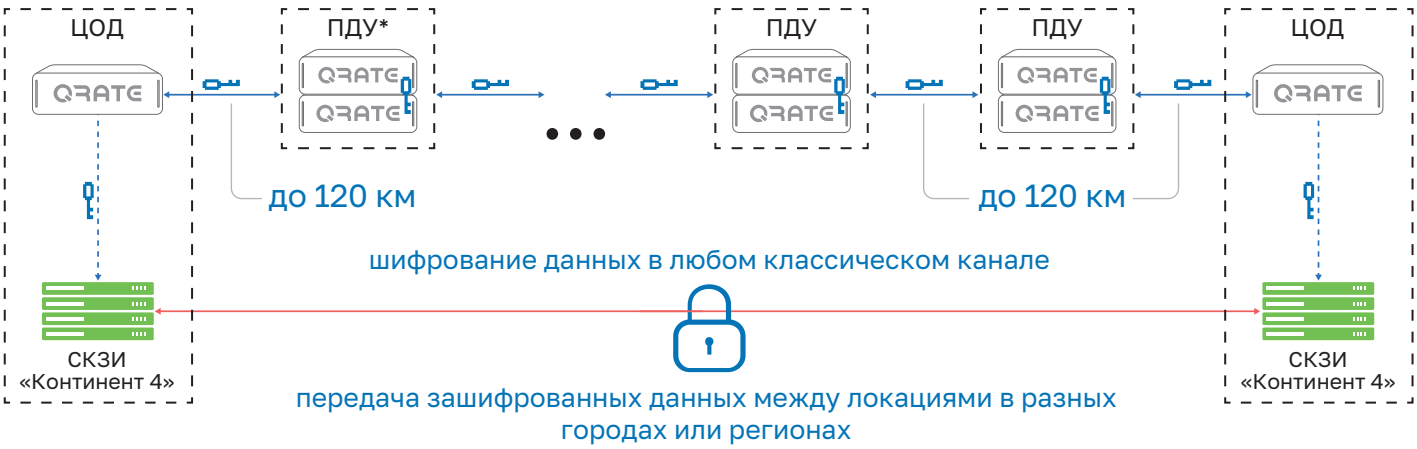
В этой связи QRate совместно с «Код Безопасности» реализуют технологию смешивания ключей, при которой ключ с систем КРК используется для усиления классического ключа с ЦУС «Континент». Подобный подход позволяет нивелировать недостаток скорости генерации ключей систем КРК, а также кратно увеличить криптостойкость VPN-шлюза «Континент», использующего полученный в результате смешивания ключевой документ.

Особенности технологии

- Высокая криптостойкость шифрования;
- Возможность оперативно заметить появление стороннего элемента в канале распределения ключевой информации;
- Простая и «мягкая» интеграция на уже работающую информационную инфраструктуру информационной безопасности;
- Возможность автономно накапливать квантовые ключи шифрования;
- Полная автоматизация процесса распределения ключевой информации даже для IIoT;
- Возможность реализации различных топологий сети;
- Использование с различными технологиями (блокчейн);
- Отказоустойчивое решение квантового распределения ключей.

Варианты использования

- Создание защищенной корпоративной сети передачи данных с использованием алгоритмов ГОСТ;
- Защита магистральных каналов связи;
- Защита трафика систем видео-конференц-связи;
- Защита каналов связи между ЦОД.



* ПДУ - промежуточный доверенный узел.

Опыт внедрения

Активное внедрение технологии в UTM Континент 4 началось в 2021 году.
Первый пилот с применением технологии квантового распределения ключей на базе Континент 4 проведен в интересах госкорпорации «Росатом». Протяжённость квантовой сети между центрами обработки данных для тестирования технологии составила 1 километр.

Первым аэропортом, протестировавшим технологию квантового распределения ключей шифрования, стал «Шереметьево». Квантовая сеть протяжённостью 5,5 километра связала «Терминал F» и «Центр обработки данных».

В 2021 году также запущена первая в России опытная квантовая сеть с открытым доступом, созданная в рамках работ консорциума Центр компетенций НТИ “Квантовые коммуникации” НИТУ МИСиС в партнерстве с МТУСИ. Сейчас она объединяет МТУСИ и МИСиС, в которых расположены пять доверенных узлов. В сети используются аппаратно-программные комплексы Кода Безопасности Континент 4 - для шифрования данных и QRate - для квантового распределения ключей. Сеть открыта для расширения и масштабирования через присоединение других учебных заведений и промышленных организаций.

Участники квантовой сети

КОД безопасности

+7 (495) 982-30-20
info@securitycode.ru
www.securitycode.ru

QRATE
QUANTUM SOLUTIONS

+7 (495) 114-55-17
mail@goqrate.com
www.goqrate.com

МТУСИ
Московский технический университет связи и информатики

+7 (495) 957-77-31
mtuci@mtuci.ru
www.mtuci.ru

МИСиС
Университет науки и технологий

+7 (495) 955-00-32
press@edu.misis.ru
www.misis.ru