



ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ И РОССИЙСКИЕ ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ: ПЕРВЫЙ ПОДХОД

Антон Гугля, руководитель

Сергей Гребнев, ведущий криптограф-исследователь

Структурное подразделение «КуАпп» Российского квантового центра

[QApp.tech](https://qapp.tech)



РОССИЙСКИЙ КВАНТОВЫЙ ЦЕНТР — УНИКАЛЬНАЯ НАУЧНО-ТЕХНОЛОГИЧЕСКАЯ ЭКОСИСТЕМА РФ

КУАПП — СПИН-ОФФ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ:

- **Трансфер технологий и коммерциализация**
- **Фундаментальные научные исследования**
- **Популяризация науки**

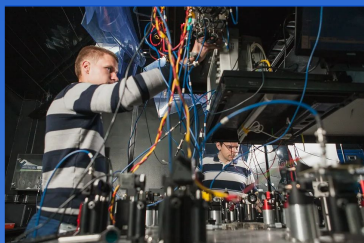
НАУЧНО-ТЕХНОЛОГИЧЕСКИЕ СФЕРЫ:

- **Постквантовая криптография**
- **Квантовые коммуникации**
- **Квантовые вычисления**
- **Квантовые сенсоры**

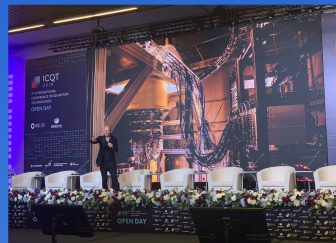
Открыт в 2010 году

900+ научных публикаций

8 спин-оффов



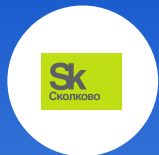
300+ сотрудников
14 научных групп
15 современных лабораторий



Российский квантовый центр является организатором регулярной конференции по квантовым технологиям ICQT

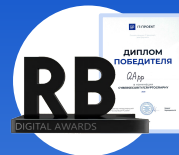
КУАПП — РАЗРАБОТЧИК ПРОГРАММНЫХ РЕШЕНИЙ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

УНИКАЛЬНЫЕ ПРОДУКТЫ ДЛЯ РЫНКА ИБ РФ



Резидент
Сколково

Научная деятельность
поддержана Российским фондом
фундаментальных исследований



КуАпп является лауреатом
премий и победителем
всероссийских конкурсов
перспективных ИТ-решений

14 сотрудников

5 объектов интеллектуальной
собственности

Более 30
научных публикаций

2 программных продукта
и полный комплекс услуг

О НАС ПИШУТ

nature

MIT
Technology
Review

PHYS.ORG

ХАЙТЕК

habr

КВАНТОВАЯ УГРОЗА ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



С помощью квантовых компьютеров злоумышленники могут атаковать данные, защищенные традиционными методами

Распространенные сегодня алгоритмы криптографии неустойчивы к квантовой угрозе

Распределение ключей	Асимметричное шифрование	Электронная подпись
ECDH DH	RSA	ECDSA DSA ГОСТ Р 34.10-2012

4098
кубит

позволяют взломать популярную криптосистему RSA-2048¹

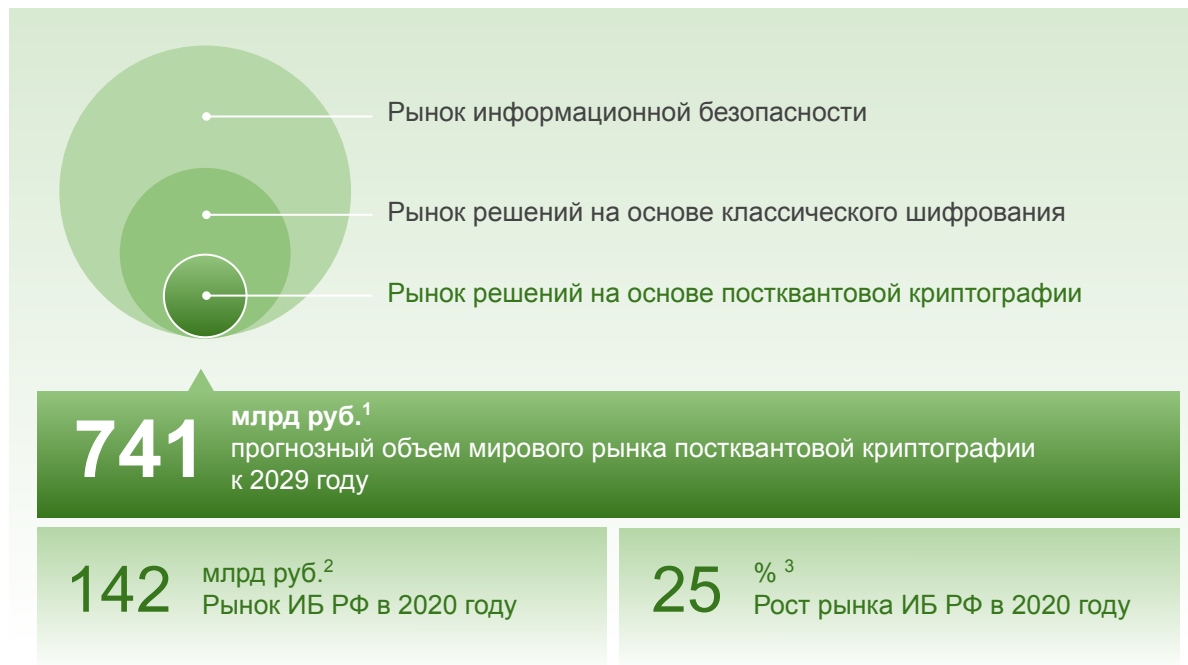


ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

Постквантовая криптография — набор алгоритмов асимметричной криптографии, взлом которых с помощью квантовых компьютеров невозможен.

Имеет те же интерфейсы, что и текущие (классические) решения асимметричной криптографии и сопоставимые нефункциональные характеристики (скорость работы, размеры ключей).

РЫНОК РЕШЕНИЙ ИБ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ НАБИРАЕТ ОБОРОТЫ



ЗАЩИЩАЕМЫЕ ДАННЫЕ

- Персональные данные
- Финансовые данные
- Медицинские и генетические данные
- Коммерческая и государственная тайна
- Данные интернета вещей
- Блокчейн-проекты

Источники: [1] Inside Quantum, [2] Anti-Malware, [3] IB Bank

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ УЖЕ ПИЛОТИРУЕТСЯ ВЕДУЩИМИ МЕЖДУНАРОДНЫМИ КОМПАНИЯМИ И СТАНДАРТИЗИРУЕТСЯ ПРОФИЛЬНЫМИ АГЕНТСТВАМИ

МИР



Крупные международные технологические компании запустили пилотные проекты



NIST

Близок к завершению 3й этап международного процесса NIST по разработке стандартов постквантовых алгоритмов

РОССИЯ



TK
26

В 2019 году ТК26 запустил процесс разработки стандартов по постквантовой криптографии в РФ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ИНТЕГРАЦИИ ПРОДУКТОВ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

ВНУТРЕННИЕ КОММУНИКАЦИИ	БОЛЬШИЕ ДАННЫЕ	ИНТЕРНЕТ ВЕЩЕЙ	БЛОКЧЕЙН-ПРОЕКТЫ	ДРУГИЕ НАПРАВЛЕНИЯ
<p>Виртуальные каналы связи</p> <p>Аутентификация</p> <p>Электронный документооборот</p> <p>Хранение данных</p>	<p>Защита данных в процессе передачи</p> <p>Гомоморфное шифрование</p>	<p>Защита программных и аппаратных компонент:</p> <ul style="list-style-type: none"> - IoT-шлюзы - IoT-облако 	<p>Защита базы транзакций квантово-устойчивыми подписями</p> <p>Квантово-устойчивые смарт-контракты</p>	<p>Атрибутное шифрование</p> <p>Конфиденциальные кооперативные вычисления</p> <p>Квантовая генерация случайных чисел</p>

РЫНКУ НЕОБХОДИМЫ КАК СВЯЗУЮЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ,
ТАК И КОНЕЧНЫЕ ПРОДУКТЫ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

КЛЮЧЕВЫЕ ПРОДУКТЫ КУАПП АКТИВНО РАЗВИВАЮТСЯ И ПИЛОТИРУЮТСЯ

PQLR SDK

DEV B2B

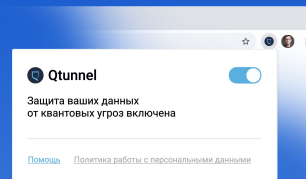


Библиотека постквантовых алгоритмов
и средства интеграции

6 Постквантовых алгоритмов

QTUNNEL

B2B B2B2C B2G



Защищенное соединение
в сетях различных топологий



Поддержка Google Chrome

НАШИ ПРОДУКТЫ УЖЕ ПРОХОДЯТ ПИЛОТИРОВАНИЕ



ГАЗПРОМБАНК

s•terra®

QRCITE

Genotek

PQLR SDK — ИНТЕГРИРОВАННАЯ С OPENSSL БИБЛИОТЕКА КВАНТОВО-УСТОЙЧИВЫХ АЛГОРИТМОВ

Отечественная реализация перспективных постквантовых алгоритмов

Кроссплатформенность и портируемость	Реализации постквантовых алгоритмов	Интеграция с OpenSSL	Простота работы	Надежность и безопасность	Поддержка отечественных решений
Linux on x86-64, ARM v7 Windows 2012+, on x86-64 Android ARM v7 Байкал-М ARM v8	Saber (Module-LWR based key exchange) Falcon (Lattice-based) McEliece (Code-based) XMSS / XMSS^{MT} (Hash-based) SPHINCS+ (Hash-based) NewHope (Lattice-based) Rainbow (MPC-based)	OpenSSL 1.0.2 1.1.0 1.1.1 TLS 1.3 1.2	Библиотека написана на языке С без зависимостей Код хорошо документирован	Теоретическая валидация Тестирование имплементации Обновления выходят 1-2 раза в месяц	Наша библиотека включает вариант ЭЦП на базе российской хэш-функции ГОСТ Р34.11-2012 «Стрибог» Реализация перспективных отечественных алгоритмов (Крыжовник, Форзиция) в самых ближайших планах

МЫ АКТИВНО РАБОТАЕМ НА ФОРМИРУЮЩЕМСЯ РЫНКЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

РАБОТАЕМ С БИЗНЕСОМ



Реализован пилотный проект по портированию нашего продукта PQLR SDK Core на платформу «**Байкал**»



Проведено успешное тестирование продукта Qtune! в интересах **Газпромбанка** для защиты host-to-host соединений с внешними клиентами Банка



Совместно с компанией **С-Терра** на базе продукта PQLR SDK разрабатывается новый продукт — «квантово-устойчивый TLS-шлюз»



Проведена пилотная интеграция квантово-устойчивых алгоритмов в решения квантового распределения ключей производства **КуРЭйт**



СОТРУДНИЧАЕМ С РЕГУЛЯТОРОМ

Являемся активными участниками подгруппы по постквантовым криптографическим механизмам технического комитета **TK26**.

Целью работы является разработка технологических стандартов по постквантовой криптографии для РФ.

РЕАЛИЗОВАН ПИЛОТНЫЙ ПРОЕКТ ПО ПОРТИРОВАНИЮ НАШЕГО ПРОДУКТА PQLR SDK CORE НА ПЛАТФОРМУ «БАЙКАЛ»

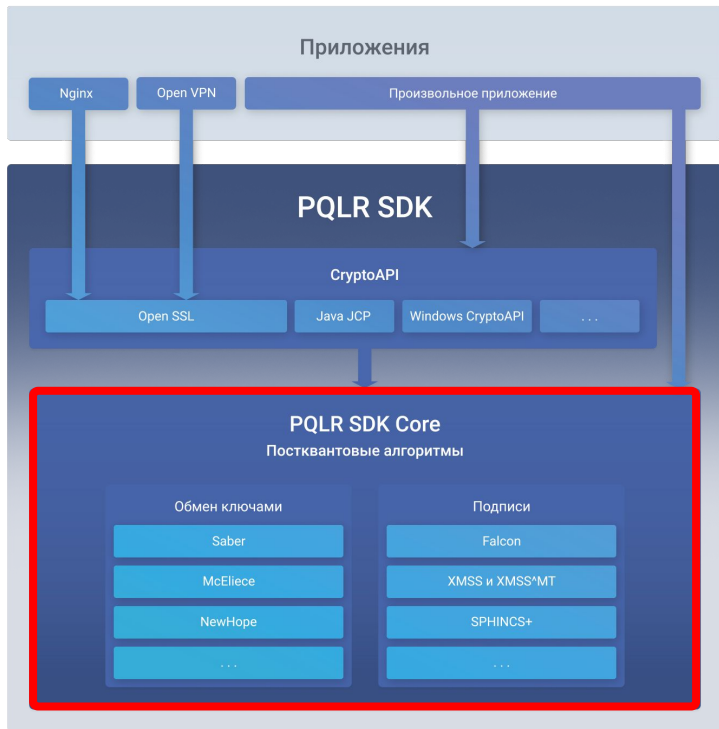


Архитектура	aarch64
Порядок байт	Little Endian
CPU(s)	8
On-line CPU(s) list	0-7
Thread(s) per core	1
Ядер на сокет	8
Сокетов	1
NUMA node(s)	1
ID производителя	ARM
Модель	3
Имя модели	Cortex-A57
Степпинг	r1p3
CPU max MHz	1500,0000
CPU min MHz	500,0000
VogoMIPS	100.00
L1d cache	32K
L1i cache	48K
L2 cache	1024K
L3 cache	8192K
NUMA node0 CPU(s)	0-7
Флаги	fp asimdv evtstrm crc32

Байкал М1000 –
микропроцессор общего
назначения с низким
энергопотреблением:

- настольные ПК
- серверные решения
- промышленные системы
- сетевое оборудование

РЕАЛИЗОВАН ПИЛОТНЫЙ ПРОЕКТ ПО ПОРТИРОВАНИЮ НАШЕГО ПРОДУКТА PQLR SDK CORE НА ПЛАТФОРМУ «БАЙКАЛ»



14 часов чистого времени

Занял процесс портирования библиотеки без платформенно-специфических оптимизаций

Корректно завершились все тесты для реализованных алгоритмов

```

baikal@baikal:~/bench/build/pqc/cpp/rainbow/test$ ./pqlr_rainbow_test | tail
[ OK ] RainbowReferenceTestGroup/RainbowReferenceTest.keygen_reference_data_test/27 (18476 ms)
[ RUN ] RainbowReferenceTestGroup/RainbowReferenceTest.keygen_reference_data_test/28
[ OK ] RainbowReferenceTestGroup/RainbowReferenceTest.keygen_reference_data_test/28 (18475 ms)
[ RUN ] RainbowReferenceTestGroup/RainbowReferenceTest.keygen_reference_data_test/29
[ OK ] RainbowReferenceTestGroup/RainbowReferenceTest.keygen_reference_data_test/29 (18477 ms)
[-----] 30 tests from RainbowReferenceTestGroup/RainbowReferenceTest (260965 ms total)

[-----] Global test environment tear-down
[=====] 118 tests from 20 test cases ran. (266543 ms total)
[ PASSED ] 118 tests.
  
```

Запуск юнит-тестов алгоритма Rainbow

ЗАМЕРЫ ПРОИЗВОДИТЕЛЬНОСТИ: ЦИФРОВАЯ ПОДПИСЬ

Вывод: постквантовые криптоалгоритмы, пригодные для использования на современных десктопных процессорах, также пригодны и для использования в системах на базе «Байкал-М»

«Байкал-М» 1.5 GHz

- ОС AstraLinuxSE 8.3.0-6
- Версия ядра 5.4.0-71-generic
- Фреймворк Google benchmark

NIST level III	KeyGen (ms)	Sign (ms)	Verify (ms)
Falcon	54.7046	2.0316	0.0893
Rainbow	7248.6475	53.4170	59.2129
SPHINCS+ (SHA256)	49.9205	1286.7593	73.5352
SPHINCS+ (Streebog) ¹	110.8631	2852.7894	165.6751

Intel Core i7-7500U CPU 2.7GHz

- ОС Ubuntu Linux 20.04
- Версия ядра 5.4.0-65
- Фреймворк Google benchmark

NIST level III	KeyGen (ms)	Sign (ms)	Verify (ms)
Falcon	22.0308	0.5325	0.0290
Rainbow	2981.7022	23.4093	25.7915
SPHINCS+ (SHA256)	16.3200	421.160	24.0646
SPHINCS+ (Streebog) ¹	23.6117	610.4588	35.4194

[1] Инициатива КуАпп по проверке применимости ГОСТ хэш-функций в постквантовых алгоритмах

ЗАМЕРЫ ПРОИЗВОДИТЕЛЬНОСТИ: ИНКАПСУЛЯЦИЯ КЛЮЧА

Вывод: постквантовые криптоалгоритмы, пригодные для использования на современных десктопных процессорах, также пригодны и для использования в системах на базе «Байкал-М»

«Байкал-М» 1.5 GHz

- ОС AstraLinuxSE 8.3.0-6
- Версия ядра 5.4.0-71-generic
- Фреймворк Google benchmark

NIST level III	KeyGen (ms)	Encaps (ms)	Decaps (ms)
NewHope	0.6698	0.9275	0.1249
McEliece	17520.6466	8.9856	396.5647
McEliece-f	5747.3424	8.9901	528.9872
SABER	0.5308	0.6953	0.8313

Intel Core i7-7500U CPU 2.7GHz

- ОС Ubuntu Linux 20.04
- Версия ядра 5.4.0-65
- Фреймворк Google benchmark

NIST level III	KeyGen (ms)	Encaps (ms)	Decaps (ms)
NewHope	0.1382	0.2303	0.0375
McEliece	1332.8600	1.9997	149.0187
McEliece-f	276.2602	2.1966	149.0123
SABER	0.0626	0.0734	0.0779

В РЕЗУЛЬТАТЕ ПРОЕКТА ПОЛУЧЕН СЕРТИФИКАТ СОВМЕСТИМОСТИ НАШЕГО ПРОДУКТА PQLR С ПРОЦЕССОРАМИ «БАЙКАЛ»



СЕРТИФИКАТ СОВМЕСТИМОСТИ

Настоящий сертификат подтверждает совместимость и корректность работы


библиотеки квантово-устойчивых криптоалгоритмов PQLR с процессорами «Байкал»

Сертификат выдан на основании испытаний,
проведенных специалистами АО «Байкал Электроникс» и «КуАпп»
(Структурное подразделение Российского квантового центра, ООО «МЦКТ»)



Компания разработчик получает право использовать
знак «Протестировано Байкал» в рекламных материалах
про указанный в настоящем сертификате продукт

г. Москва
14.03.2022


Виталий Богданов
Директор по развитию
АО «БАЙКАЛ ЭЛЕКТРОНИКС»

НАШЕ ВИДЕНИЕ ПО РАЗВИТИЮ НАПРАВЛЕНИЯ

- Расширение списка поддерживаемых криптоалгоритмов: приоритетная реализация алгоритмов ГОСТ Р 34
- Портирование PQLR на другие перспективные платформы: Эльбрус, RISC-V, MIPS, роутеры
- Оптимизация постквантовых криптоалгоритмов под конкретные архитектуры
- Профилирование реализаций, выявление узких мест
- Предложения по расширению набора инструкций и созданию специализированных криптографических сопроцессоров
- Интеграция в TPM-решения

МЫ ОТКРЫТЫ К СОТРУДНИЧЕСТВУ

Направление №1

3х-сторонние пилотные проекты
QApp - Байкал - Ваше решение

Направление №2

Пилотные проекты
QApp - Ваше решение

ГОТОВЫ ПРЕДОСТАВИТЬ PQLR SDK ДЛЯ ТЕСТИРОВАНИЯ

МЫ ОКАЗЫВАЕМ ПОЛНЫЙ КОМПЛЕКС УСЛУГ
ПО ЗАЩИТЕ ОТ КВАНТОВЫХ УГРОЗ

АУДИТ ИС
И ТРЕНИНГИ ПО ИБ

СТРАТЕГИЯ
ЗАЩИТЫ

АРХИТЕКТУРА
КОНЕЧНЫХ
РЕШЕНИЙ

ПОСТАВКА НАШЕГО
ПО, ИНТЕГРАЦИЯ
И ПОДДЕРЖКА

ЕСЛИ СЕГОДНЯ ВЫ ВПЕРВЫЕ УСЛЫШАЛИ СЛОВА «ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ»



«[ЧТО ТАКОЕ ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ](#)» на сайте Яндекс.Кью



«[БАЗА ЗНАНИЙ](#)» на сайте QApp

СПАСИБО ЗА ВНИМАНИЕ



ЗАЩИЩАЕМ ОТ КВАНТОВЫХ УГРОЗ

Антон Гугля

Руководитель

+7 925 537-71-53

apg@rqc.ru

Сергей Гребнев

Ведущий исследователь

+7 910 469-91-26

s.grebnev@rqc.ru

Максим Кот

Ведущий разработчик

mkot@qapp.tech

При поддержке



[QApp.tech](https://qapp.tech)

ДАННЫЕ С ДЛИННЫМ ЖИЗНЕННЫМ ЦИКЛОМ МОГУТ ПРЕДСТАВЛЯТЬ НАИБОЛЬШУЮ ЦЕННОСТЬ ДЛЯ АТАКУЮЩЕГО

ИМЕННО ИХ НУЖНО ЗАЩИЩАТЬ В ПЕРВУЮ ОЧЕРЕДЬ ОТ КВАНТОВОЙ УГРОЗЫ

Оптимальный момент чтобы начать тестировать решения информационной безопасности на основе постквантовой криптографии

Жизненный цикл защищенных данных

Злоумышленник реализует атаку «Сохранение данных сейчас — взлом потом»

2021 2022 2023 2024 2025 2026 2027 2028 2029 2030

2030

Появляется универсальный квантовый компьютер способный взломать традиционные алгоритмы криптографии

[Узнать больше про квантовую угрозу](#)

ЦЕННОСТЬ ДЛЯ КЛИЕНТА

ПРОДУКТЫ ИБ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ — ОПТИМАЛЬНЫЙ МЕТОД ЗАЩИТЫ ДАННЫХ ОТ КВАНТОВОЙ УГРОЗЫ

**Квантовая угроза усиливает
ключевые риски ИБ по ряду
направлений**



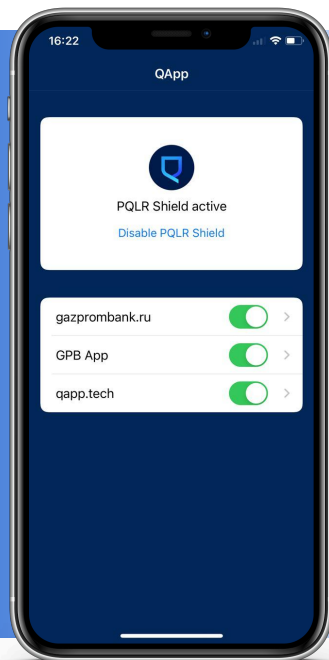
Сетевая
инфраструктура



Стандартное программное
обеспечение



Промышленный
и потребительский
Интернет вещей



Продукты КуАпп надежно защищают ценные
данные бизнеса и государства от квантовой угрозы

- Кроссплатформенность и портбельность
- 6 актуальных постквантовых алгоритмов
- Интеграция от 1 дня в базовых сценариях
- Регулярные обновления
- Гибкие модели лицензирования
- Вендорская техническая поддержка

Предусмотрен вариант ЭЦП
на базе Российской криптографической хэш-функции

Возможна поставка продуктов КуАпп
в составе комплекса КРК КуРэйт

ОТЛИЧИЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ОТ КВАНТОВОЙ

Является полностью программным решением асимметричной криптографии.

Позволяет оставить архитектуру системы неизменной — не требует привнесения аппаратной части или изменения протоколов.

Позволяет сохранять мобильность с меньшими затратами — портирование портативного ПО обычно, дешевле модификации производственных линий.

Имеет менее сильное доказательство стойкости — используются математические выкладки базирующиеся на знании об известных алгоритмах для квантовых и классических компьютеров, принципах их устройства и известных методах проведения атак, в отличие от аксиом квантовой физики на основе которых строится доказательство устойчивости для квантовой криптографии.

Не расширяет возможностей классических, асимметричных алгоритмов — например, без использования аутентификации невозможно избежать MITM атак при распределении ключей, соответственно протоколы типа TLS остаются актуальными.

СИНЕРГИЯ ПОСТКВАНТОВОЙ И КВАНТОВОЙ КРИПТОГРАФИИ

ПРИМЕРЫ СЦЕНАРИЕВ

Последняя миля —

доставка ключей до потребителей не включенных непосредственно в квантовую сеть

PKI (инфраструктура открытых ключей) —

поддержка аутентификации между различными сегментами квантовых сетей или организация доступа к ключам

Защита вспомогательных соединений от MITM атак —

в результате MITM не получится скомпрометировать ключ, но можно вызвать более сложно отлаживаемый отказ в обслуживании