РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Использование смарт-карт для распределения квантово-защищенных ключей

РусКрипто

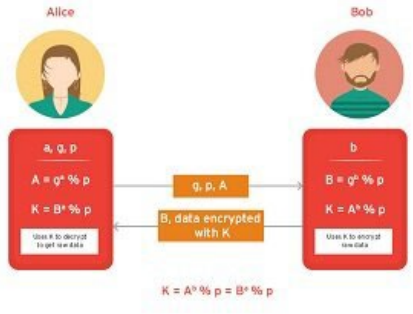
Андрей Кузнецов
АО «НИИМЭ»

Так ли всё плохо с классической криптографией?

РусКрипто

- Протокол **Диффи-Хеллмана** уязвим – известен алгоритм атаки с применением квантового компьютера и алгоритма Шора
- Схема Диффи-Хеллмана и подобные ей сейчас применяется при **распределении ключей**

Вывод: нужны другие схемы **распределения ключей**



Квантовый компьютер

Какие есть решения?

РусКрипто

- **Квантовое распределение ключей** (КРК) использует физический принцип для распределения ключей, нет никакого обратного преобразования

- Пост-квантовые криптографические алгоритмы, в частности, пост-квантовое расширение Диффи-Хеллмана **PQXDH**

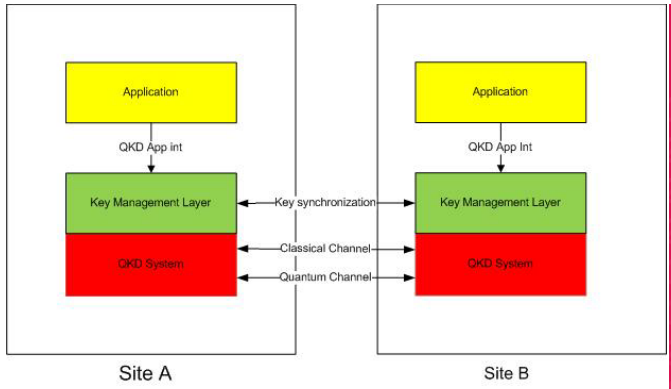
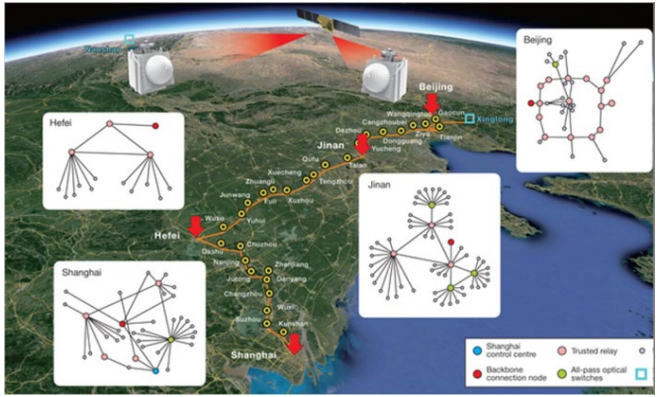


Схема интерфейса КРК-внешнее приложение из ETSI GS QKD 004

Системы квантового распределения ключей

РусКрипто

- Технология для получения одинаковых симметричных ключей на двух узлах
- Может быть расширена для получения согласованных ключей на N > 2 узлах сети (см., например, российские протоколы ISTOQ и ProtoQa)
- Требует соединения конечных узлов КРК оптоволокном



Квантовая сеть в Китае. Суммарная длина ~4600 км. Иллюстрация из статьи Chen, YA., Zhang, Q., Chen, TY. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).

Проблема «последней мили»

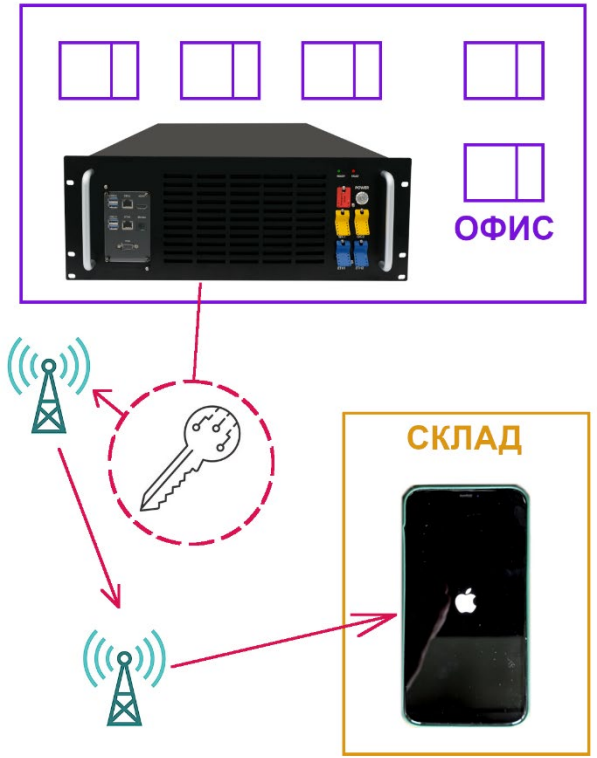
- Пользовательское устройство может не быть напрямую связано с узлом КРК

РусКрипто

Проблема «последней мили»

- Пользовательское устройство может не быть напрямую связано с узлом КРК
- Пользовательское устройство может находиться вне доверенного контура
- Пользовательское устройство может иметь другой класс защиты

Вопрос: как ключ попадает из узла сети КРК в целевое СКЗИ (телефон, ПК и т.п.) вне доверенного контура и без использования привычных схем распределения ключей?



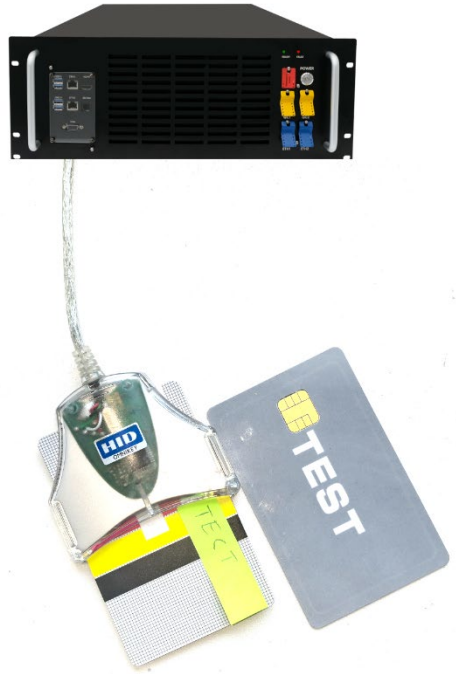
РусКрипто

Где хранить квантово-защищенный ключ?

РусКрипто

Специализированная **карта-токен:**

- Получает актуальные мастер-ключи с терминала, подключенного к КРК, внутри доверенного контура
- Вычисляет сессионные ключи оффлайн
- Обеспечивает аутентификацию пользователя (PIN-код)
- Поддерживает защищённый обмен сообщениями (ЗОС) при общении с целевым СКЗИ вне доверенного контура



Сценарий: «квантовый мессенджер»

- В организации есть несколько филиалов, соединённых сетью КРК
- Работники получают мастер-ключи на свои карты-токены на проходной
- В мессенджере 3 режима:

1) чат
2) групповой чат
3) электронная почта

- Конкретная реализация мессенджера не обсуждается в данном докладе

РусКрипто

Выработка сессионных ключей

- Алгоритм должен вырабатывать уникальные сессионные ключи
- Параметры сессии не являются секретом и согласовываются по открытому каналу
- Сессионные ключи доступны только непосредственным участникам чата или переписки

KDF$_{TREE}$ из **P50.1.113-2016**

Протокол обмена: ISO 7816-4
ЗОС с взаимной аутентификацией и выработкой сессионных ключей по **P50.1.113-2016**

$$SKM = KDF_{TREE}[64](K_{in}, LABEL_{SKM}, SEED)$$
$$K_{CCS} = KDF(K_{in}, LABEL_{CCS}, SEED)$$
$$SEED = TimeStamp \mid ID_1 \mid ID_2 \mid ... \mid ID_N$$

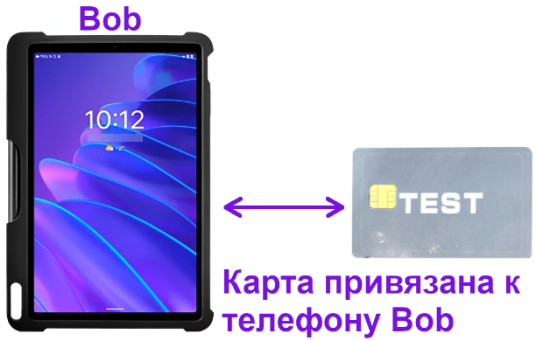
РусКрипто

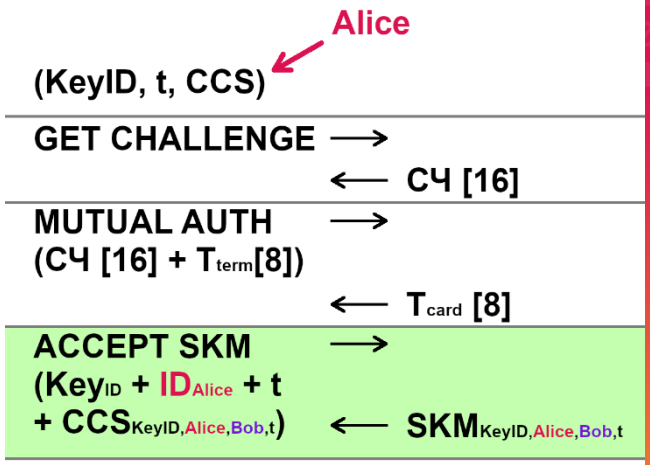
Особенности протокола

- Для успешной установки ЗОС с токеном терминал должен запросить PIN-код.
- Выработка ключей контролируется токеном – только сессии, в которых участвует владелец токена.
- Токен контролирует возрастание временной метки

Особенности протокола

- Для успешной установки ЗОС с токеном терминал должен запросить PIN-код.
- Выработка ключей контролируется токеном – только сессии, в которых участвует владелец токена.
- Токен контролирует возрастание временной метки и выход за пределы разрешённого временного окна.
- Токен проверяет подпись входящих запросов на переписку.





РусКрипто

Принципиальная схема установки сессии

РусКрипто

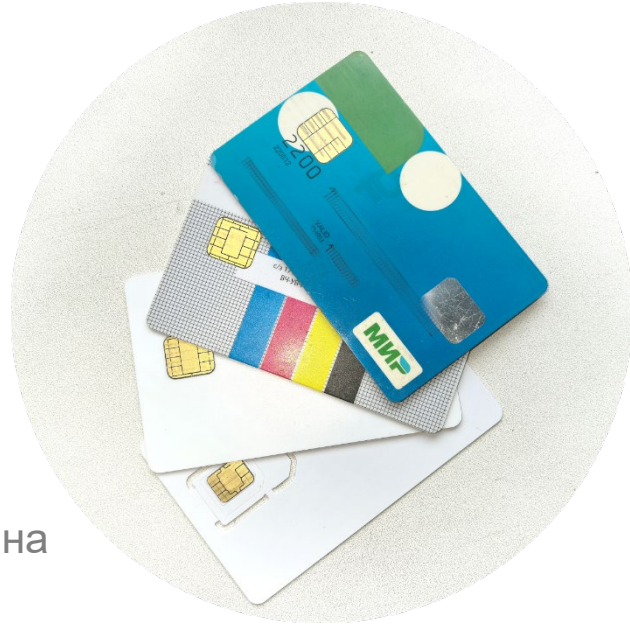
Alice (инициатор сессии)	Bob
Подготовка данных сессии, ввод PIN-кода для работы с токеном.	
Получение **СКМ** и **подписи** от токена для группы (+Bob) и временной метки t0.	
Формирование пакета авторизации и отправка абоненту Bob.	Извлечение открытых параметров сессии, ввод PIN-кода от токена.
	Выработка **СКМ** на токене для группы (+Alice) и t0 с проверкой **подписи**.
Проверка криптограммы с использованием **СКМ**.	Проверка пакета авторизации. Отправка ответной криптограммы.
Сессия считается установленной, на обеих сторонах вычислен одинаковый **СКМ** = $KDF_{TREE}(K_{master}, LABEL_{SKM}, ID_A \mid ID_B \mid t0)$	

Что может предложить АО «НИИМЭ»?

РусКрипто

Прототип токена для «квантового мессенджера» разработан в **НИИМЭ** на базе смарт-карты с ОС Just 2.00, произведенной на заводе **Микрон**.

- JavaCard API расширен за счет поддержки российских криптографических алгоритмов.
- Имеется аппаратное ускорение российских криптографических алгоритмов (для хэширования по ГОСТ Р34.11-2012 ускорение на 2 порядка по сравнению с программной реализацией)



РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ