Квантовые сети и доверенные промежуточные узлы: сетевые протоколы распределения ключей

Алексей Уривский

infotecs

КРК: основы

- Две абонента генерируют по случайной битовой строке
- Выполняется протокол обмена квантовыми состояниями и их обработки
- Выбираются совпадающие части строк – выработка общего секрета
- Достижение безопасности требует аутентификации передаваемых данных

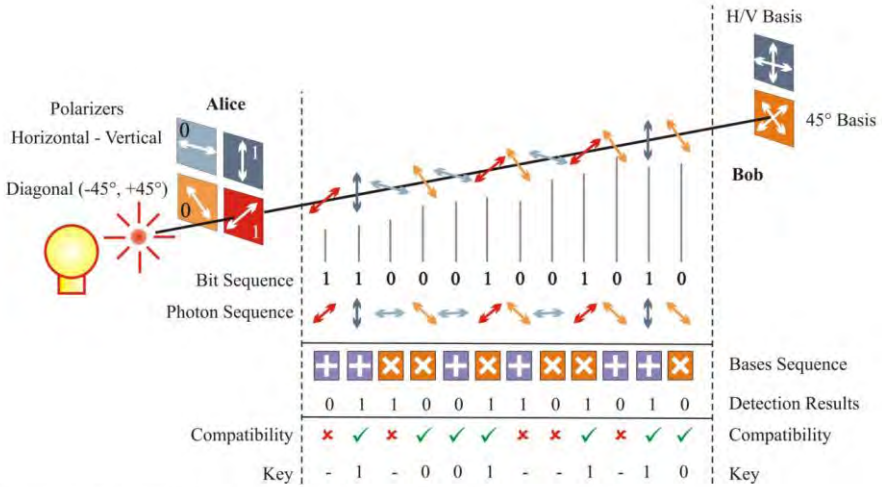
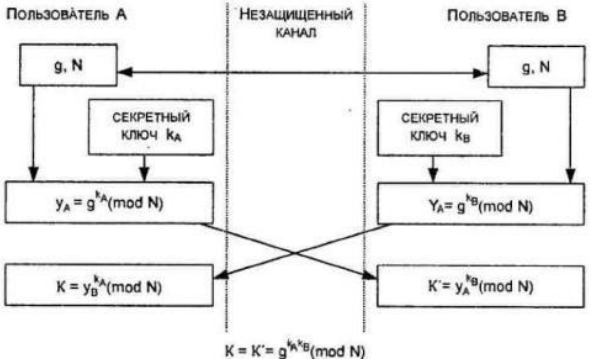


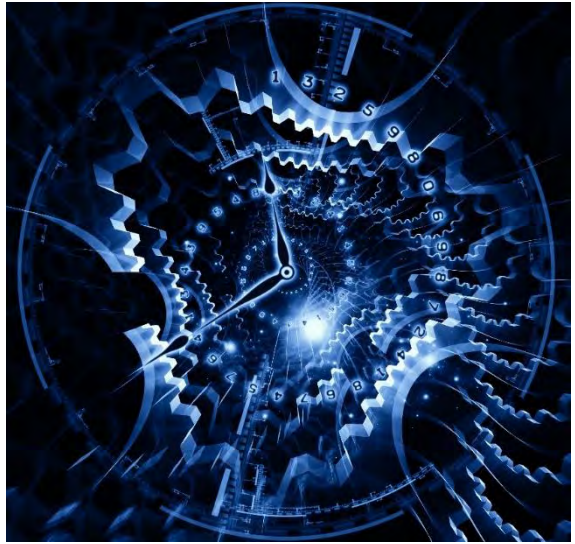
Fig. 1. Key exchange in the BB84 protocol implemented with polarization of photons (adapted from [56]).

КРК и протокол Диффи-Хеллмана

- **Функциональная эквивалентность**
- **Неэквивалентность**
  - Разная способы выработки общего секрета
  - Стойкость в разных моделях
  - Реализуемость: **без ограничений по расстоянию для DH, ограниченное расстояние для КРК**



Увеличение расстояния для КРК: прямое увеличение



Более качественные компоненты

- волокно с меньшим поглощением
- сверхпроводящие детекторы
- истинно однофотонные источники

Практический предел

- 400 км в оптоволокне
- 150 км свободное пространство

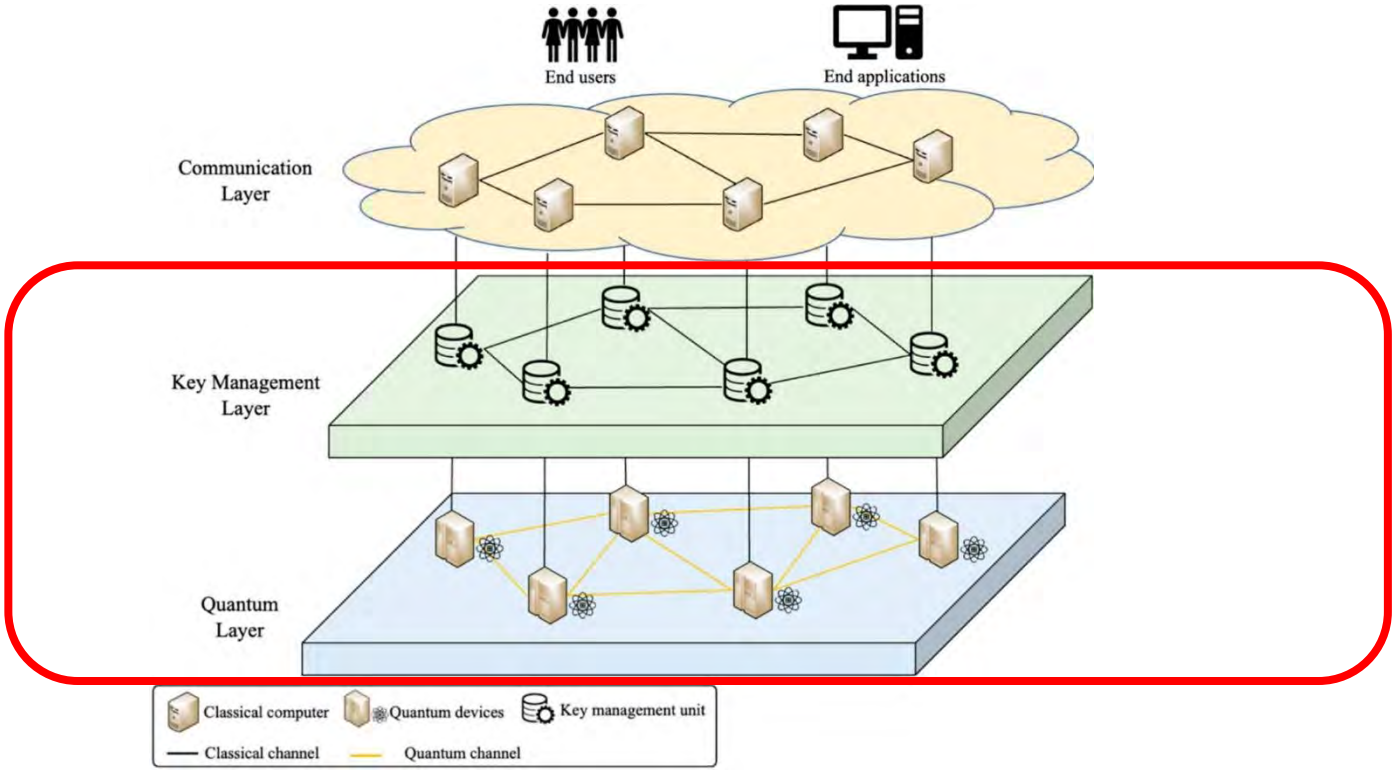
Низкая скорость выработки ключа

Увеличение расстояния: сети КРК

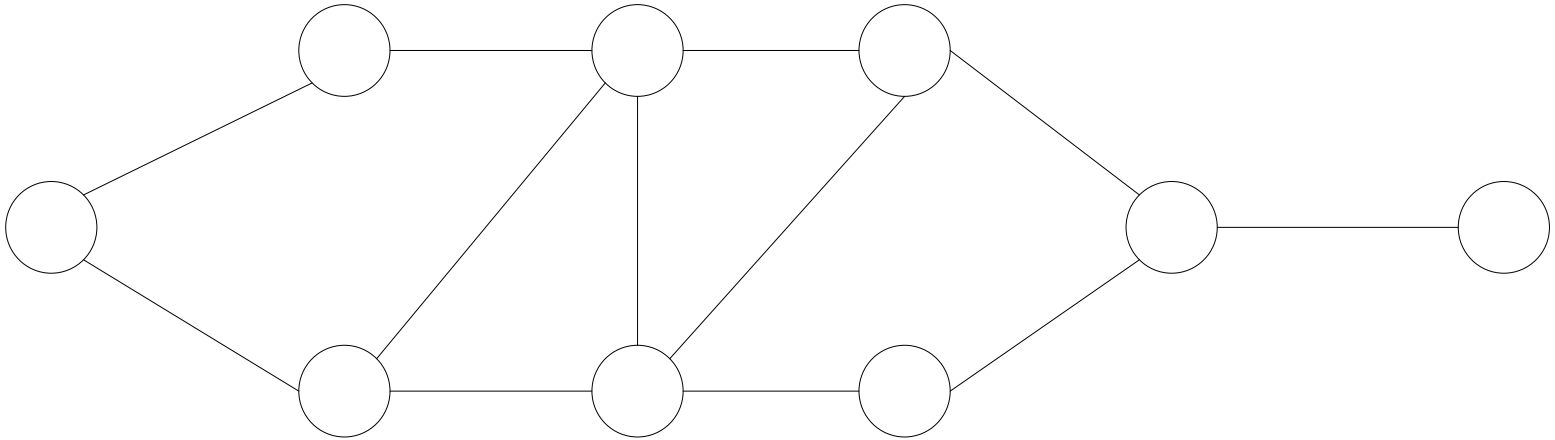
Сеть КРК – совокупность квантовых узлов (аппаратуры), некоторые из которых, обычно географически соседние, связаны между собой квантовым каналом,
такая, что несвязанные прямым квантовым каналом узлы могут выработать общий секретный (квантовый) ключ.

- математическая модель – граф;
- вершина – квантовый узел;
- ребро – квантовый канал.

Сеть КРК

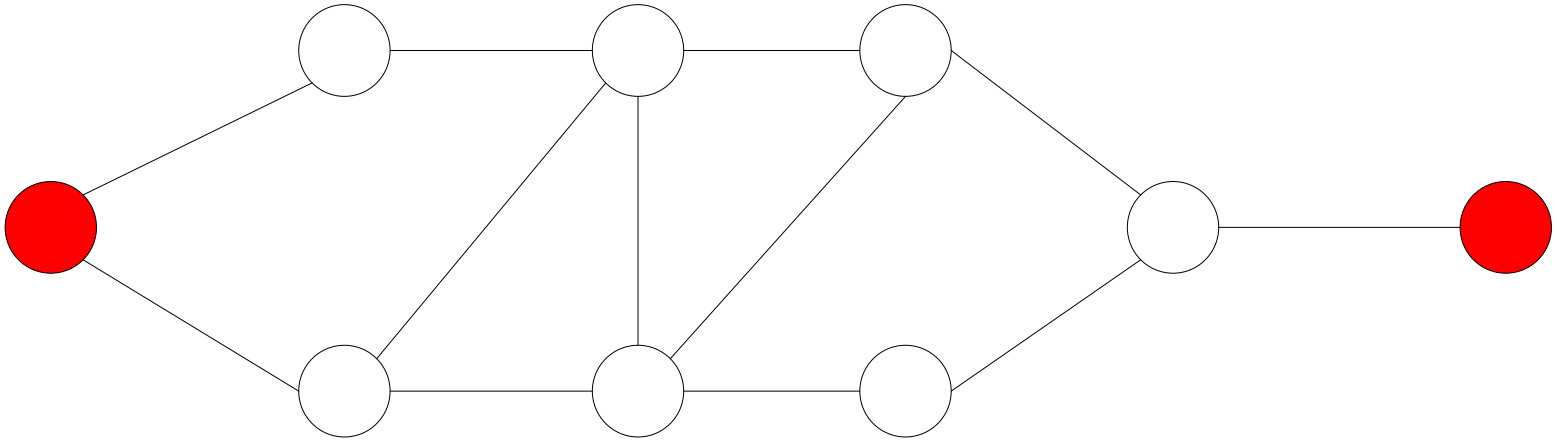

End users
End applications
Communication Layer
Key Management Layer
Quantum Layer
Classical computer
Quantum devices
Key management unit
Classical channel
Quantum channel

Сеть КРК



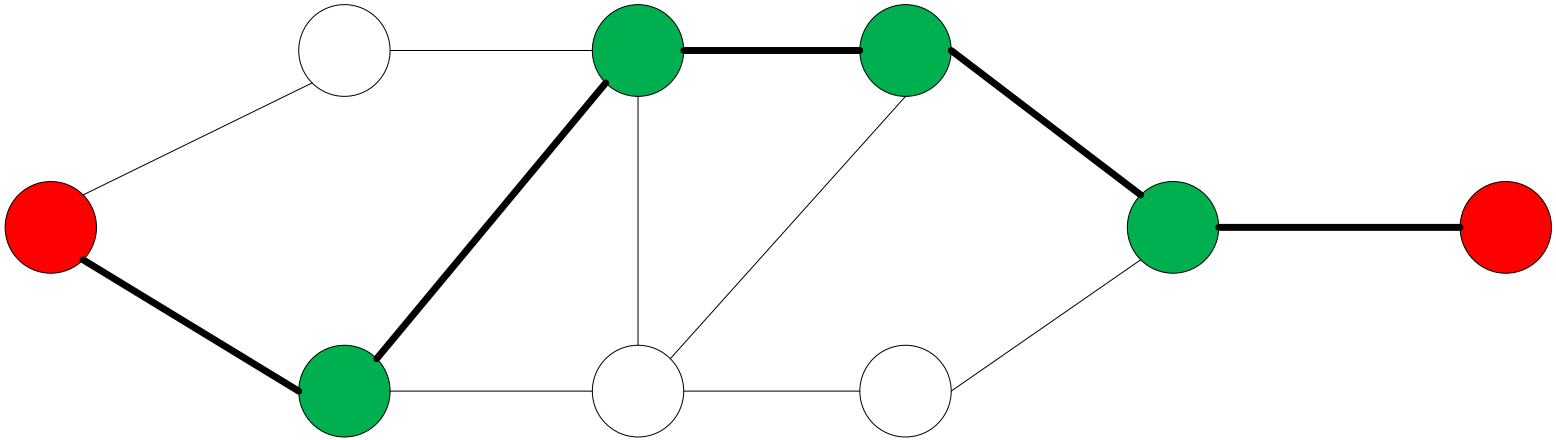
Сеть КРК

Целевые абоненты



Сеть КРК

Маршрут (квантовый путь)



Сеть КРК

Задача: выработать общий ключ между целевыми абонентами

Структура сети КРК

Связная сеть КРК – для каждой зафиксированной пары узлов в графе сети имеется квантовый путь.
Для выработки общего ключа для произвольной пары на сети достаточно уметь решать задачу на **цепочке связных** узлов: в топологии «магистраль».

Узлы сети КРК

Недоверенный узел: участвует в протоколе, некорректность операций или вмешательство злоумышленника обнаруживается сами протоколом. **Злоумышленник может иметь доступ к узлу** и его компонентам, но это не приводит к компрометации итогового ключа.

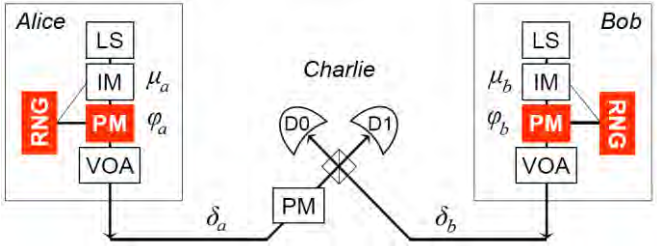
Доверенный узел: участвует в протоколе и обязан корректно выполнять предписанные действия. **Злоумышленник не должен иметь доступ к узлу** и/или его внутренним состояниям, относящимся к работе протокола.

Недоверенные узлы сети КРК – физические реализации

- Протоколы с квантовыми репитерами и квантовой памятью
- Measurement Device Independent (MDI)-протоколы
- Twinfield-протоколы

Особенности

- не доказана реализуемость или увеличение расстояния всего в 2 раза
- прецизионные изделия, аналогичные целевым узлам
- **низкая скорость выработки на больших расстояниях**



Рекорд: 833 км при поглощении в волокне 140 дБ.

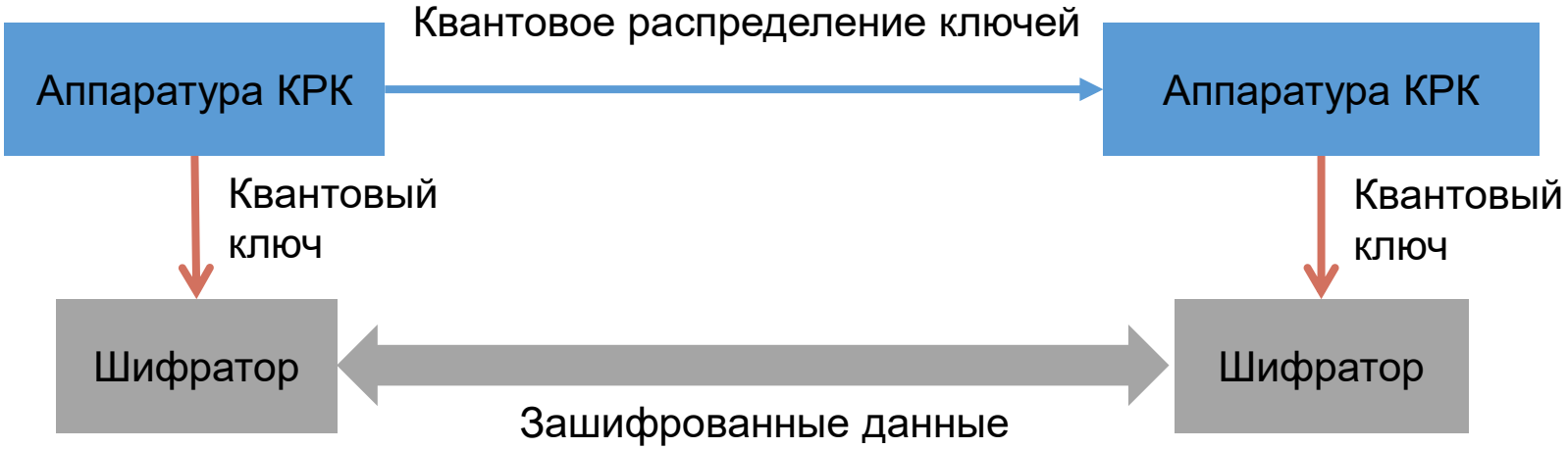
Доверенные узлы сети КРК – криптографические методы

Базовая операция на промежуточном узле

- Перешифрование трафика
- Перешифрование ключа

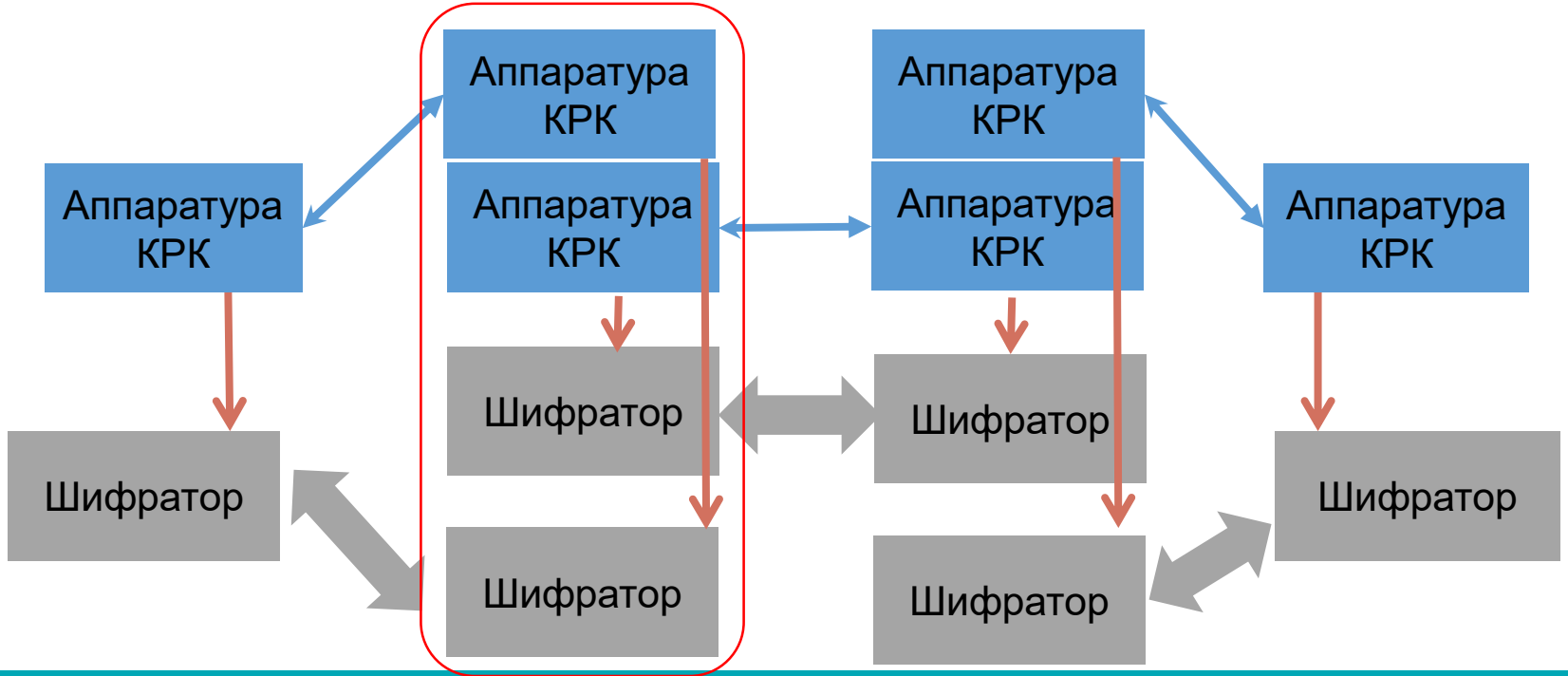
Перешифрование данных

Конечная цель использования КРК – получать для заданной пары узлов ключи для шифрования при обмене данными



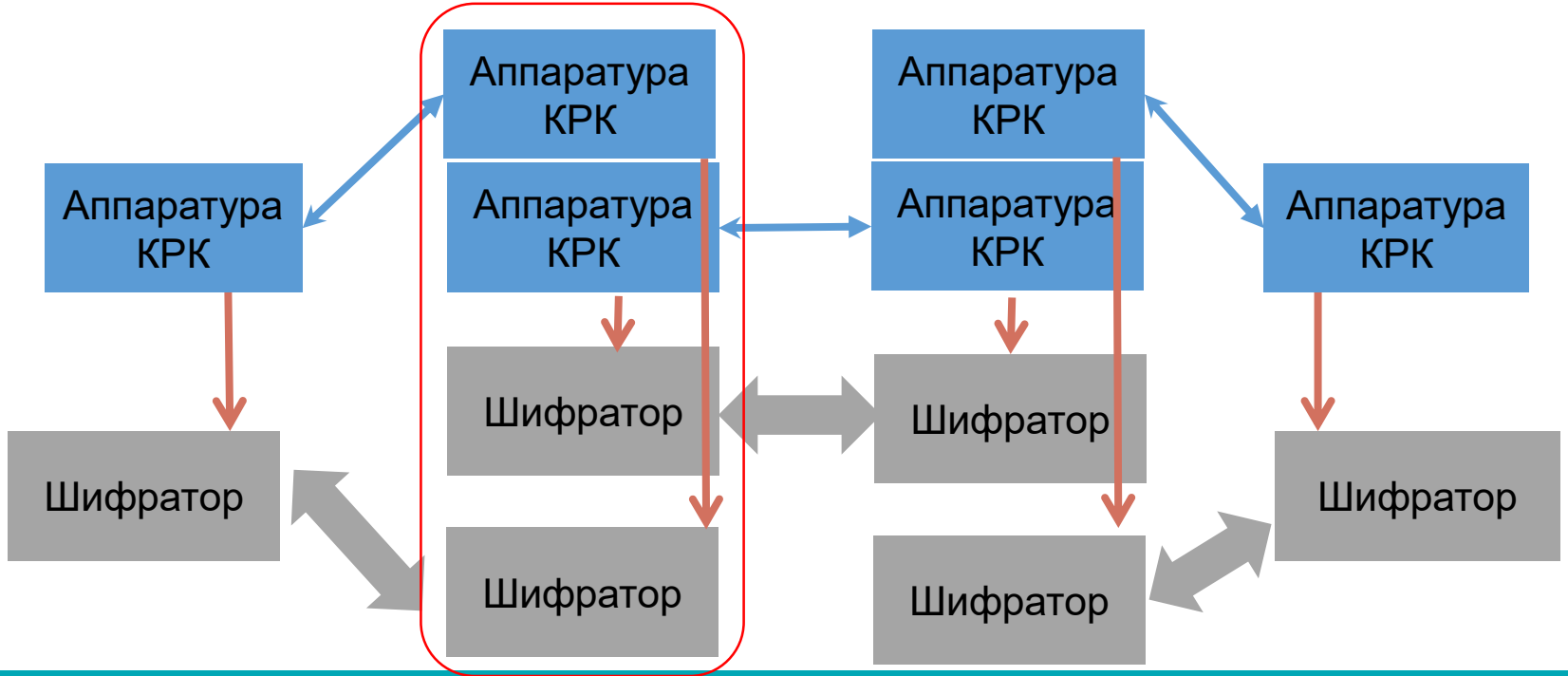
Перешифрование данных

- В каждом промежуточном узле ставим двойной комплект квантовой аппаратуры – выработка ключа с соседом справа и слева, – и двойной комплект шифраторов.



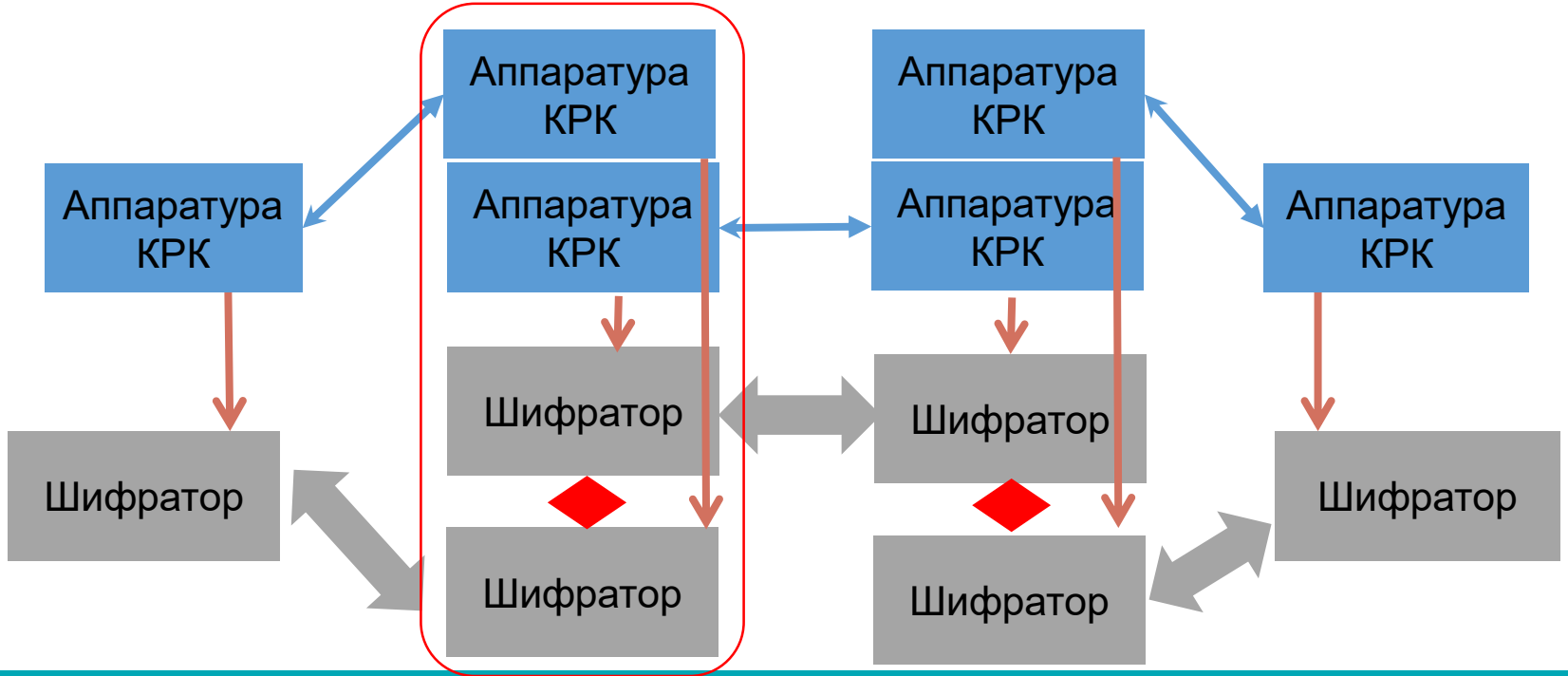
Перешифрование данных

- Квантовые ключи вырабатываются КРК на каждом линке, каждый промежуточный узел имеет два независимых ключа.



Перешифрование данных

- Защищаемые данные проходят через каждый промежуточный узел: расшифровываем при приеме на одном ключе и зашифровываем при отправке на другом.

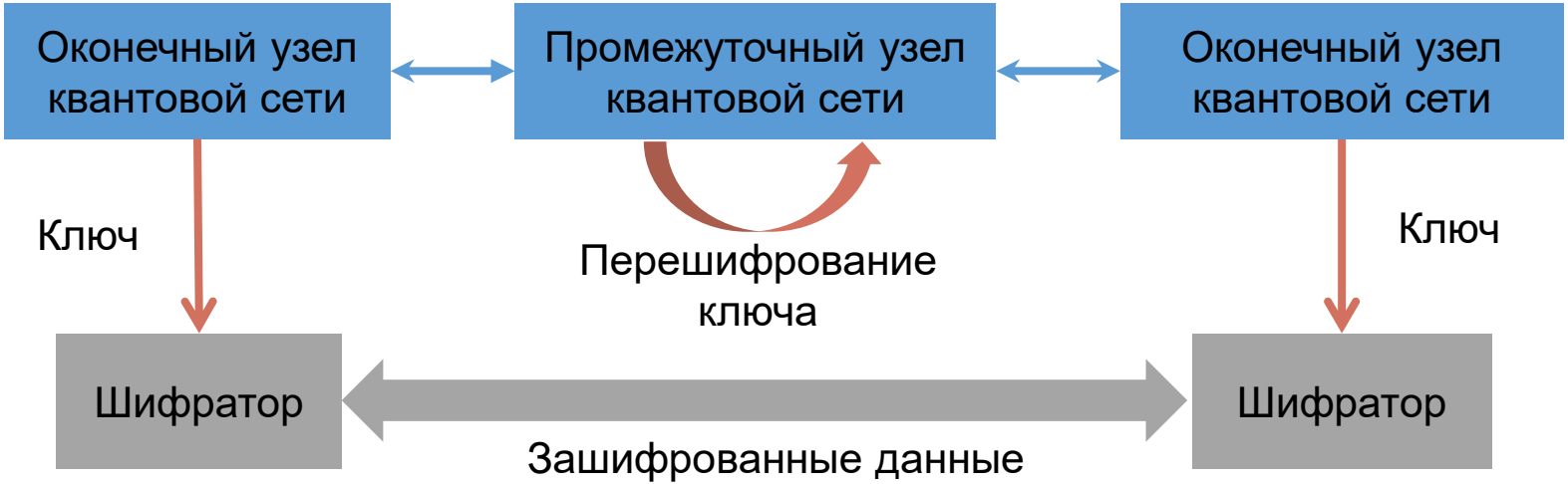


Перешифрование трафика: особенности

- На каждом промежуточном узле **два «лишних» шифратора**.
- При любом устройстве шифраторов и квантовой аппаратуры промежуточный **узел должен быть доверенным**: между двумя шифраторами есть канал, через который проходит открытый трафик.
- **Рост задержек** при передаче данных в сети: каждый шифратор вносит задержку
- Через каждый промежуточный узел должен проходить (скоростной) **канал передачи данных**.
- **Экономические эффекты**: рост стоимости, увеличение массогабаритов, потребление энергии.

Перешифрование ключа

- В каждом промежуточном узле ставим двойной комплект только квантовой аппаратуры – выработка ключа с соседом справа и слева.
- Квантовые ключи вырабатываются КРК на каждом линке, каждый промежуточный узел имеет два независимых ключа.



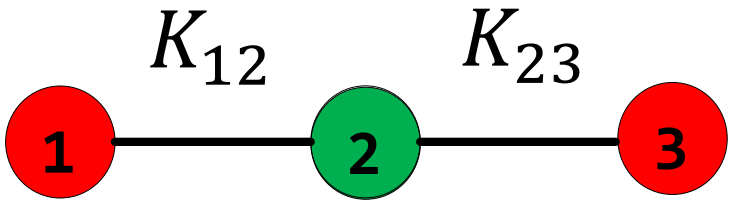
Перешифрование ключа

- Защищаемые данные через промежуточный узел могут не проходить.
- Через каждый промежуточный узел проходит будущий общий секретный ключ: расшифровываем общий ключ при приеме на одном квантовом ключе и зашифровываем при отправке на другом.

Устранены все недостатки схемы с перешифрованием данных, кроме доверенности промежуточных узлов.

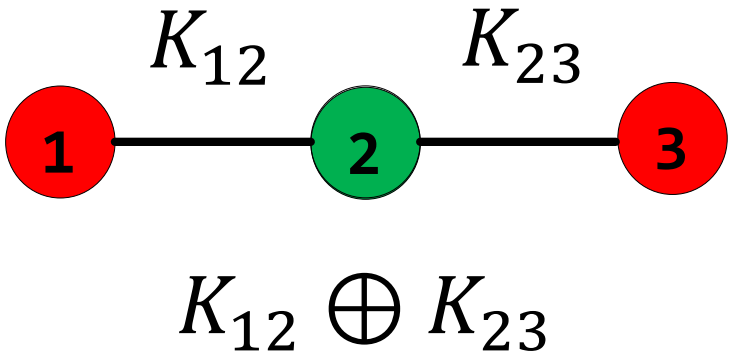
Традиционный пример: 3 узла

- Цепочка из 3 узлов. Выработаны 2 ключа: K_{12} и K_{23}.
- Оба ключа доступны промежуточному узлу.



Традиционный пример: 3 узла

Промежуточный узел вычисляет $K = K_{12} \oplus K_{23}$
и отправляет его в открытый канал.

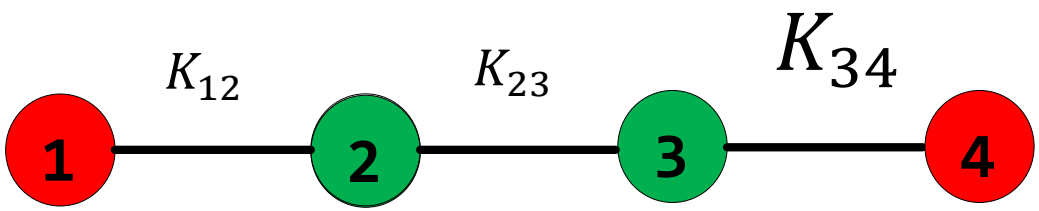


Традиционный пример: 3 узла

- Каждый из крайних узлов может получить как K_{12}, так и K_{23}. Любой из этих ключей можно считать общим ключом. Пусть K_{12}.
- Если оба ключа K_{12} и K_{23} «идеальные», то K_{12} абсолютно стойкий: K есть результат зашифрования K_{12} на секретной ключе K_{23}в режиме одноразового блокнота, т.е. абсолютно стойкого шифра.

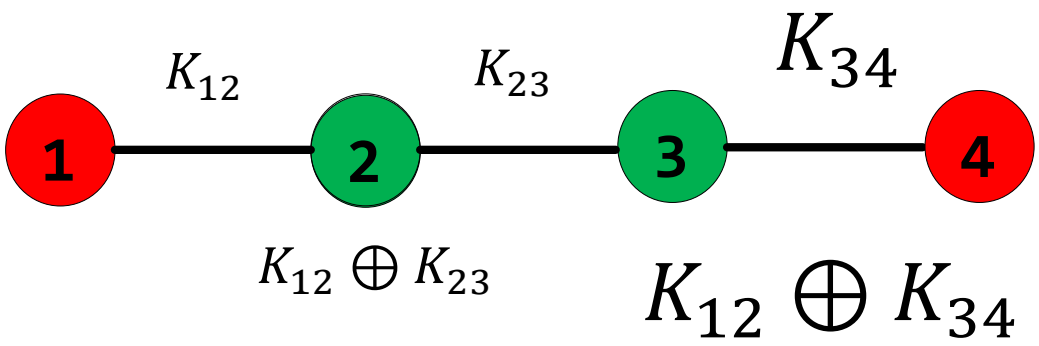
Обобщение традиционного примера: случай 4 узлов

Добавим 4 узел. Он станет крайним узлом, а предыдущий крайний узел станет промежуточным. Появится новый ключ K_{34}.



Обобщение традиционного примера: случай 4 узлов

- Узел 3 отправит в канал $K_{12} \oplus K_{34}$.
- Все узлы в цепочке имеют общий ключ K_{12}.



Обобщение традиционного примера: случай 4 узлов

Особенность: для узла 4 ключ K_{12} просто случайная двоичная строка, которая поступила зашифрованной на ключе K_{34}.

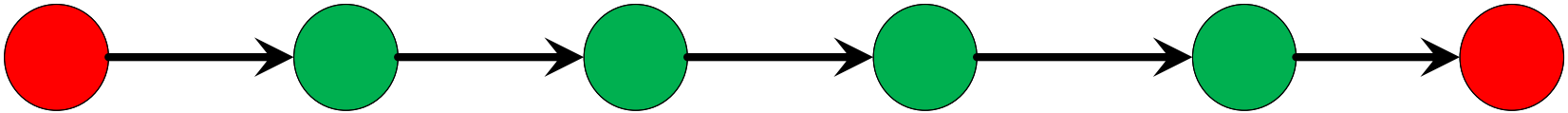
Он получает будущий общий ключ в зашифрованном виде, перешифровывает его и передает дальше по цепочке.

При этом промежуточный узел уже никак не влияет на ключ K_{12}, считая его просто случайным числом.

Он выступает релеем и выполняет **защищенный транспорт (безопасную передачу)** секретного ключа.

Общий случай: произвольное число узлов.

- Все узлы в цепочке имеют общий ключ K_{12} и для всех кроме первых двух это случайная двоичная строка, передаваемая в канале зашифрованной на некотором квантовом ключе.
- Каждый промежуточный узел выступает релеем и выполняет **защищенный транспорт (безопасную передачу) секретного ключа.** Иногда говорят – «проталкивает» секретный ключ по цепочке.



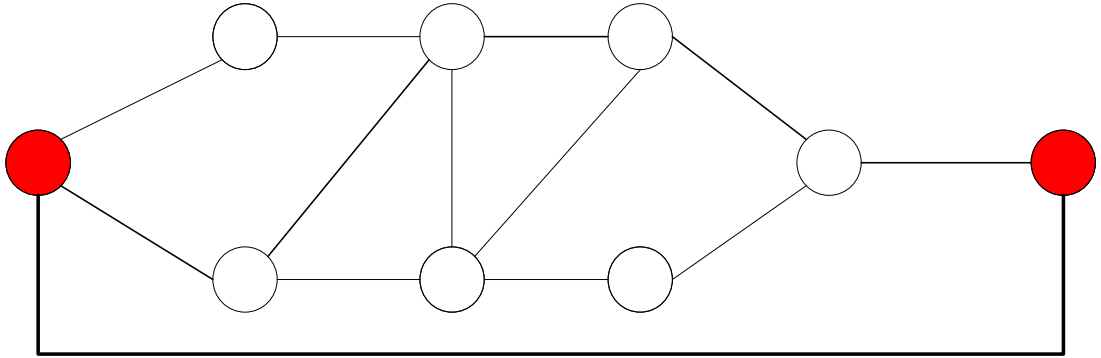
Защищенный транспорт ключа: общий случай.

- Один из оконечных узлов, скажем 1, в цепочке генерирует случайный ключ K. Он не получен ни из какого протокола КРК. Он выбран случайно и равновероятно и всего множества ключей.
- У двух соседних узлов i и j имеется общий ключ ключ K_{ij}, выработанный в квантовом протоколе.
- i-ый узел отправляет в канал $E(K, K_{ij})$, т.е. результат зашифрования (защиты) ключа K на ключе K_{ij} с использованием функции $E(.,.)$.
- Принимающий узел перешифровывает K и отправляет дальше.
- Последний узел в цепочке расшифровывает принятое сообщение и получает K.

Квантовозащищенный ключ

- Ключ K не был выработан ни в каком протоколе КРК. Он «неквантовый».
- Ключ K защищенным образом был транспортирован по всей цепочке промежуточных узлов, при этом для его защиты использовались квантовые ключи K_{ij}.

Ключ K – **квантовозащищенный (КЗК).**



КЗК

Квантовозащищенный ключ

Ключ *K* – **квантовозащищенный.**

- Ключ K известен любому промежуточному узлу.
- При длине цепочки *L* и вероятности компрометации любого промежуточного узла *p*, вероятность компрометации квантовозащищенного ключа ~(N-2)p.

Функция защиты *E(.,.)*

- *E(.,.)* – **функция шифрования** – секретность ключа
  - одноразовый блокнот – абсолютная стойкость
  - блочный шифр в подходящем режиме работы – вычислительная стойкость.
- *E(.,.)* – **обеспечение аутентичности** ключа
  - 2-универсальные – абсолютная имитостойкость (большой расход ключа).
  - имитовставка с использованием блочного шифра в подходящем режиме работы – вычислительная имитостойкость.
  - схема цифровой постквантовой подписи – вычислительная аутентичность.

Защищенный транспорт в топологии «звезда»

- Пусть все цепочки для любой пары узлов проходят через один выделенный узел – центр «звезды».
- Центр звезды формирует квантовозащищенный ключ К.
- Центр звезды инициирует защищенный транспорт ключа К в обе стороны цепочки.

Бессмысленность КРК?

- Любой протокол КРК требует предварительно распределенного секрета – ключей для аутентификации в открытом канале.
- При любой функции аутентификации ключи аутентификации «расходуются».
- Когда ключ аутентификации будет «израсходован» его надо заменить новый. За это время будет выработано *N* квантовых ключей.
- Почему нельзя сразу вместо ключей аутентификации двум абонентам доставить *N* секретных ключей, особенно при малом *N*? Это полностью **обесценивает КРК**.

Самовоспроизводимость ключей КРК

- Тривиально: **скорость формирования квантовых ключей должна быть строго больше, чем скорость потребления ключей аутентификации.**
- Часть вырабатываемых квантовых ключей, или долю каждого ключа, будем использовать как ключи аутентификации – самовопроизводимость квантовых ключей.
- Всегда ли это верно?
  - для вычислительной стойкости – почти наверное, да;
  - для абсолютной стойкости – открытый вопрос!

«Неидеальные» ключи и механизмы в защищенном транспорте

Квантовый ключ «неидеальный», лишь **ε-секретный:** следовое расстояние между идеальным ключом и ничего незнающим подслушивателем и реальным ключом и реальным подслушивателем

$$\frac{1}{2}\left|\left|\rho_{KE} - \rho_U \otimes \rho_E\right|\right|_1 \leq \varepsilon.$$

Среднее число опробуемых ключей из всего множества N до нахождения правильного
при частичном опробовании с вероятностью успеха π

$$Q \geq \left(1 - \frac{\varepsilon}{\pi}\right)\frac{N(1-4\varepsilon)+1}{2}$$

«Неидеальные» ключи и механизмы в защищенном транспорте

- Какая ε-секретность квантовозащищенного ключа $K = K_{12} \oplus K_{23}$?
- Как меняется ε-секретность с ростом длины цепочки?
- Как меняется ε-секретность при использовании ε-почти 2-универсальной хэш-функции и идеальном ключе аутентификации? При ε-секретном ключе аутентификации?
- Как меняется ε-секретность с ростом числа сеансов аутентификации?

ε-секретность КЗК в цепочке

Если на i —ом линке цепочки выработан ε_i -секретный квантовый ключ, то ε-секретность квантовозащищенного ключа оценивается

$$\varepsilon \leq \sum_i \varepsilon_i .$$

Линейный рост ε с длиной цепочки.

ε-секретность КЗК при ε-почти 2-универсальной хэш-функции

infotecs

Если для выработки имитовставки при транспорте ε-секретного квантовозащищенного ключа используется ε_{A}-почти строго 2-универсальная хэш-функция, а в качестве ключа аутентификации – ε_K-секретный, то ε-секретность квантовозащищенного ключа

$$\varepsilon_{next} \leq \varepsilon + \varepsilon_{\mathrm{A}} + \varepsilon_K .$$

Как минимум, **линейный рост ε_{next} с числом сеансов** аутентификации.

Ограничения самовоспроизводимости для абсолютной стойкости

- ε-секретность КЗК ухудшается:
  - с ростом длины цепочки растет линейно растет;
  - при аутентификации ε_K-секретным ключом растет с числом сеансов, как минимум, линейно.
- Для фиксации ε необходимо сильнее сжимать просеянный ключ в процедуре усиления секретности. **Падает скорость выработки ключа.**

На больших расстояниях для заданного малого ε потенциально может существовать такая длина цепочки, что квантовый ключ перестанет самовоспроизводиться.

Открытый вопрос!

Выработка общего ключа

Перейдем от защищенного транспорта (=распределения) секретного ключа к его выработке – совместному формированию секретного ключа 2 абонентами.

- Оба концевых абонента в цепочке генерируют каждый свой случайный ключ K_1 и K_2.
- Выполняем два направленных навстречу друг другу защищенных транспорта.
- Вычисляем функция смешивания $KDF(K_1, K_2)$ двух независимых ключей в один секретный КЗК.

Симметризация защищенного транспорта с одинаковым вкладом обоих концевых абонентов – **выработка общего ключа.**

Требования к $KDF(.,.)$ (качественно)

- Выход $KDF(.,.)$ неотличим от случайного и равновероятного ключа при любом входе – экстрактор энтропии.
- Знание выхода не позволяет вычислить вход - однонаправленность.
- Знание части выхода не позволяет вычислить неизвестную часть выхода.
- Знание части входа не позволяет вычислить выход, если неизвестной части входа достаточно для получения выхода требуемого качества.

Варианты реализации:

- абсолютная стойкость – 2-универсальные хэш-функции;
- вычислительная стойкость - криптографические хэш-функции.

НеСтойкость КРК?

- Ряд протоколов КРК в теории доказуемо абсолютно стойкие при выполнении ряда понятных условий.
- Конкретные реализации могут быть нестойкими
  - невыполнимость условия в конкретной реализации;
  - невыполнимость условия из-за неидеальностей компонентов;
  - неконтролируемое и непредсказуемое изменение параметров компонентов при воздействии злоумышленника;
  - ухудшается ε-секретность итогового ключа.

Что будет, если **конкретная реализация** конкретного протокола КРК будет **скомпрометирована**? **Использование дополнительных ключевых систем и гибридизация ключей.**

Гибридизация ключей

- Пусть имеются 2 независимые ключевые системы: система с КРК и альтернативная.
  - распределение ключей доверенными курьерами
  - распределение ключей постквантовых механизмов.
- У двух абонентов возникает по секретному ключу от каждой из ключевых систем.
- Смешиваем два секретных ключа с использованием $KDF(.,.)$со свойствами, рассмотренными ранее – проводим **гибридизацию ключей (=cryptoagility).**

Компрометация любой из ключевых систем не приводит к компрометации итогового ключа.

infotecs

Ответы на вопросы

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363