Квантовое распределение ключей. Квантовозащищенные ключи.

Бородин Михаил

Что такое КРК?

КРК – ещё один способ распределить ключи

Распространены схемы распределения ключей

- Доставка ключей доверенным курьером
- Криптографические протоколы, использующие только алгоритмы с секретным ключом («симметричные»).
- Криптографические протоколы, использующие алгоритмы с открытым ключом.
  - Протоколы типа Диффи-Хеллмана.
  - Криптосистема RSA

Нарушитель без квантового компьютера

Схемы, способные обеспечить безопасность при нарушителе с квантовым компьютером

- Доставка ключей доверенным курьером
- Криптографические протоколы, использующие только алгоритмы с секретным ключом («симметричные»).

\+ + +

- Схемы, основанные на «постквантовых задачах» (PQC)
- **Системы, квантового распределения ключей** (QKD)

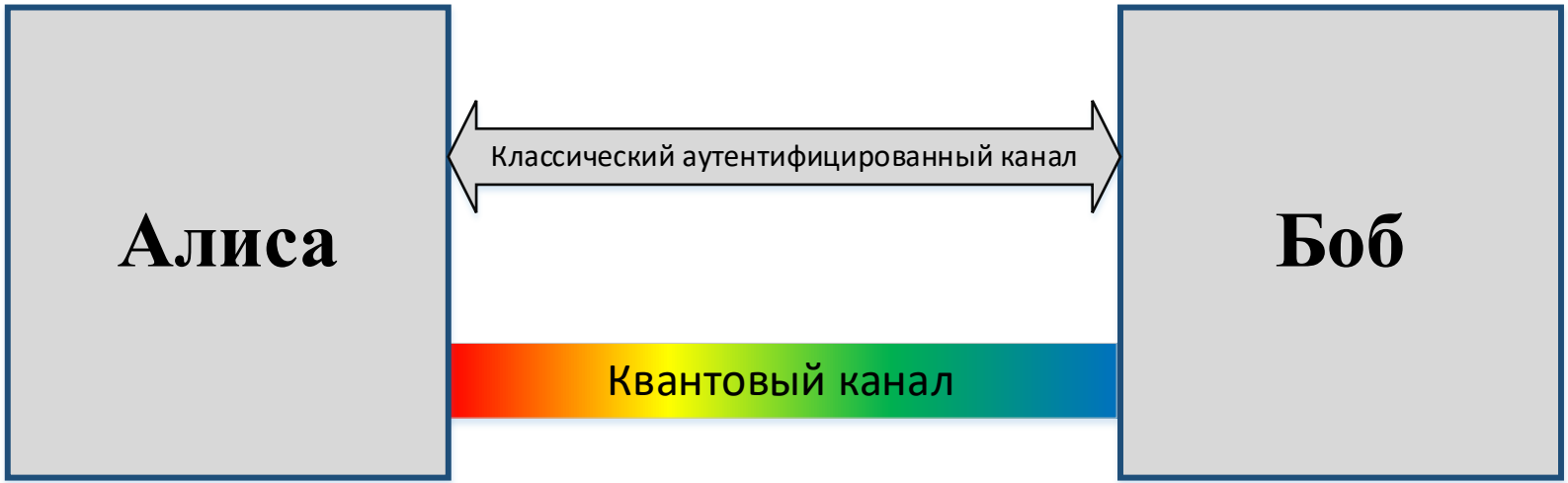
Нарушителю доступен и квантовый компьютер

Предпосылки внедрения и ожидания от использования КРК

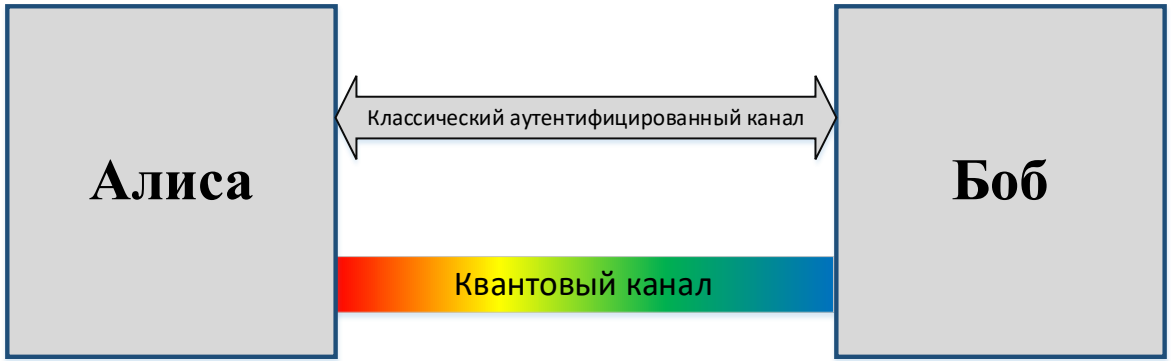
Предпосылки использования:

- Популярные методы распределения ключей, такие как «RSA» и «Диффи-Хеллман», уязвимы для нарушителя с квантовым компьютером.
- Красивая теоретическая модель:
  - «фундаментальные законы природы»;
  - «принципы неопределенности Гейзенберга»;
  - доказательство безусловной теоретико-информационной стойкости квантового протокола.
- Пилотные проекты ведущих организаций в Мире. Технология признана состоятельной. Внедрение в инфраструктуру государств.

Упрощенная модель функционирования системы КРК

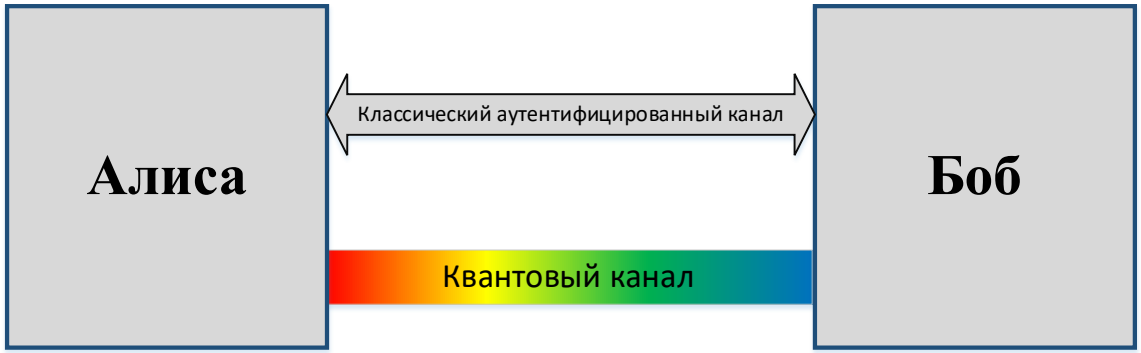


Этап отправки/приема фотонов



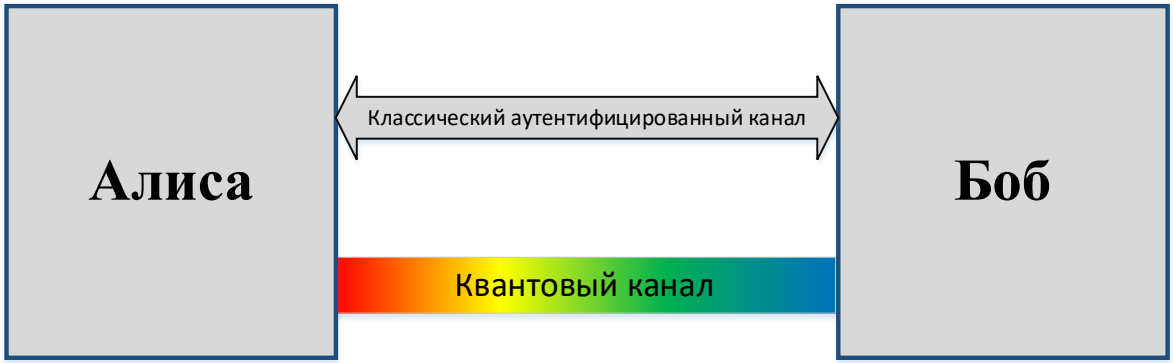
Алиса готовит квантовые состояние и отправляет их Бобу. Состояние характеризуется одним из двух базисов и передаваемым значением. Базис и значение для каждого состояния выбираются случайно.

Этап отправки/приема фотонов



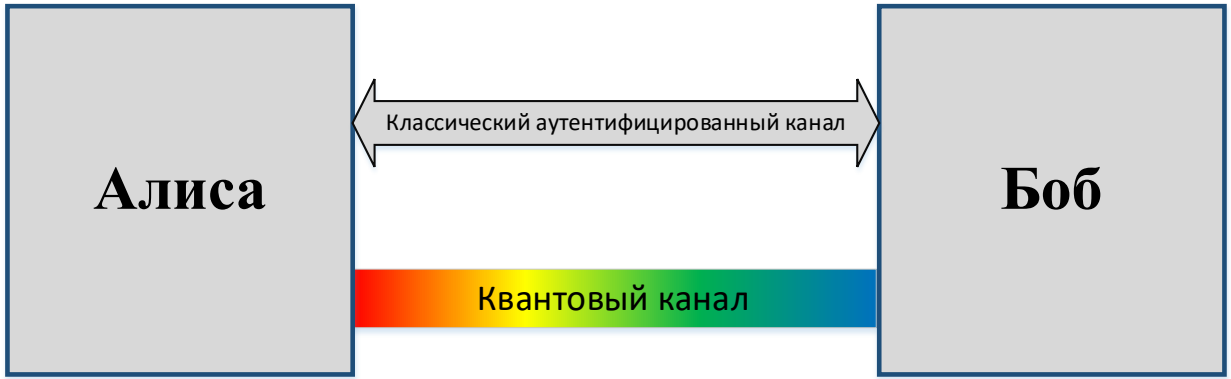
Боб случайным образом выбирает один из двух базисов и в выбранном базисе проводит измерения.

Этап просеивания

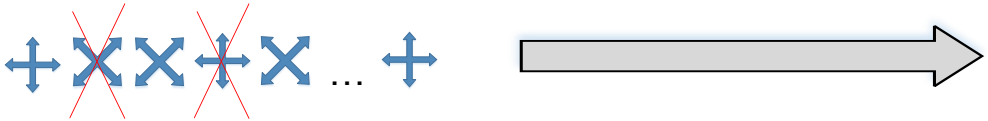


Боб сообщает Алисе, в каких базисах он проводил измерения, но не результат этих измерений:

Этап просеивания

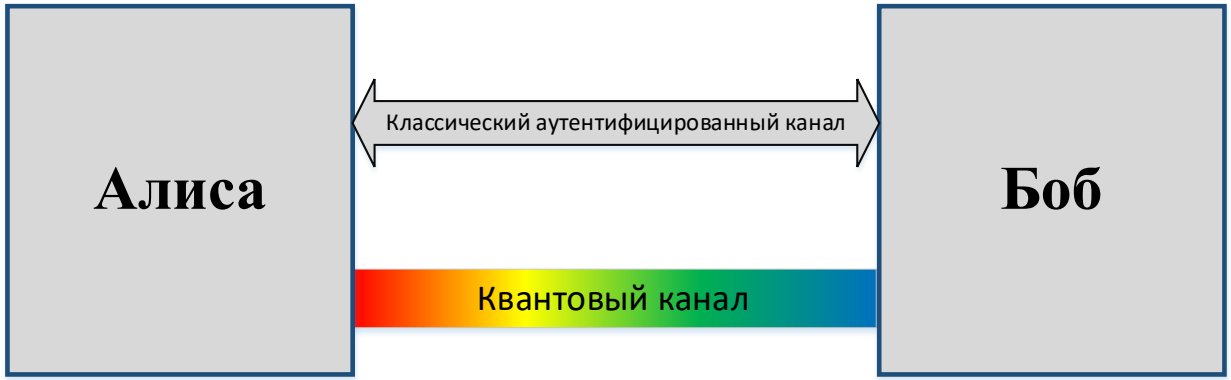


Алиса, сообщает Бобу номера фотонов, в которых
он правильно угадал базис:



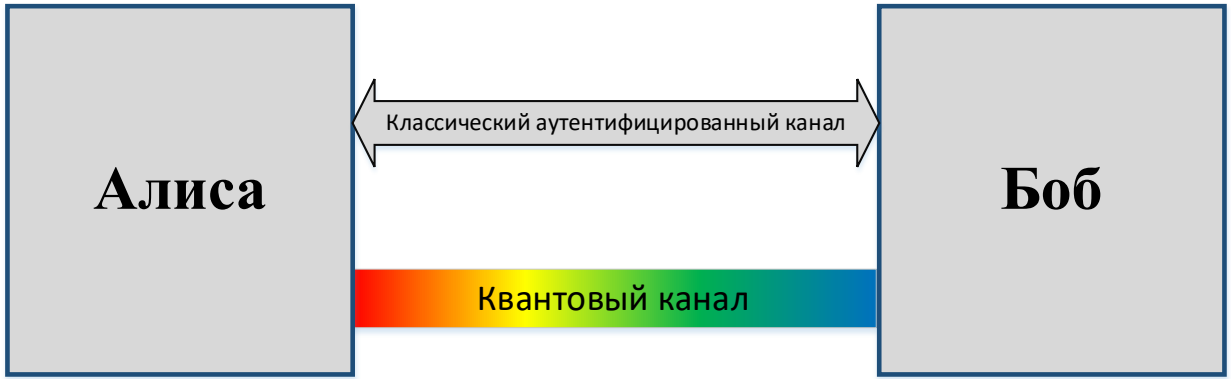
Алиса и Боб исключают из последовательности те компоненты,
которые были измерены в неправильном базисе.

Этап исправления ошибок



В идеальном случае после процедуры просеивания последовательности Алисы и Боба должны совпадать. Но на практике всегда случаются ошибки. Для их устранения применяется механизм, использующий коды исправляющие ошибки. Механизм позволяет измерить уровень ошибок, если их количество не превышает порог, то ошибки исправляются. Если порог превышен, то сеанс завершается с ошибкой.

Этап усиления секретности



Так как механизм коррекции ошибок приводит к частичному раскрытию информации о последовательности, то такую последовательность нельзя использовать в качестве секретного ключа. Последовательность подвергается процедуре сжатия, которая позволяет достичь нужных криптографических свойств у выходной последовательности.

Получившаяся выходная последовательность (или ее часть) называется **квантовым ключом**.

Суровая реальность разработки

Задачи, которые необходимо решить

infotecs

«Инженерные» задачи

- В большинстве схем нужно использовать источник одиночных фотонов.
- Защита от физических атак на аппаратуру:
  - Атаки, использующие нестрогую однофотонность источника (PNS);
  - С ложными состояниями (FSA), временными сдвигами (TSA), ослепление детекторов (DBA);
  - Троянский конь (THA);
  - и т.д.
- Уменьшения числа ошибок при передаче
  - Качество детекторов
  - Выбор среды распространения

«Криптографические» задачи

- Как обеспечить аутентифицированный канал?
  - Теоретико-информационная или вычислительная стойкость?
  - Как распределить предварительные ключи и как их обновлять?
- Исправление ошибок и усиление секретности
  - Выбор алгоритмов и значений параметров: компромисс между скоростью выработки и «секретностью» ключа.
- Использование полученных ключей в системе:
  - Как передать ключ конечному потребителю?
  - Как с использованием КРК построить сеть распределения ключей?

Как обеспечить аутентифицированный канал?

infotecs

Теоретико-информационная стойкость

Универсальные хэш-функции.

Плюсы:

- Безусловная теоретико-информационная стойкость задаваемая параметрами.

Минусы:

- Одноразовое использование ключа.
- Размер ключей (есть решения, которые зависят от размера сообщения и размера имитовставки).

Вычислительная стойкость

Известные алгоритмы имитовставки:

- HMAC
- ГОСТ Р 34.13-2015
- MGM

Плюсы:

- Допускает многократное использование ключа.
- Размер ключа не зависит от длины обрабатываемых данных.
- Алгоритм одобренный регулятором.

Минусы:

- Не обеспечивают теоретико-информационную стойкость.

Исправление ошибок и усиление секретности

Задачи, относящиеся к процессу исправления ошибок:

- Выбор кодов и их параметров для достижения наибольшей производительности при заданных условиях работы системы.

Задачи, относящиеся к процессу усиление секретности:

- Выбор алгоритмов и значений параметров: компромисс между скоростью выработки (степенью сжатия) и криптографическими свойствами ключа.

Использование квантовых ключей. Гибридизация

infotecs

Целесообразность гибридизации:

- Новая технология абсолютного доверия нет.
- Способ использования КК в качестве источника дополнительной энтропии.

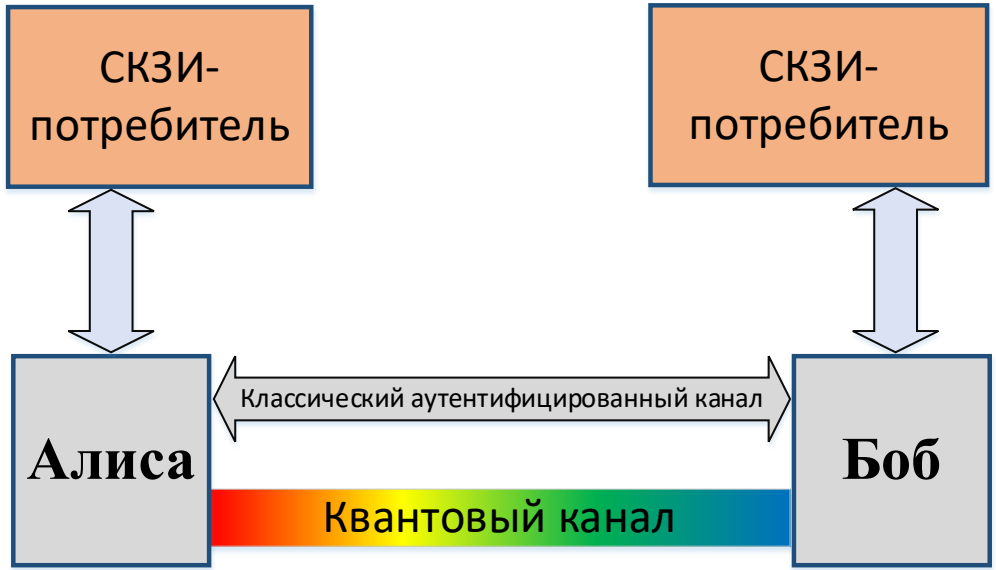
Способы гибридизации:

- XOR двух ключей. (Возможны проблемы: работа Key distribution. Episode 1: Quantum menace, G. Marshalko, V. Rudskoy)
- Функция выработки производных ключей (KDF), есть соответствующие стандарты. Что смешать?
  - Предраспределенный ключ
  - Ключ, полученный с использованием протокола Диффи-Хеллман.
  - PQC
  - КК

Гибридизация – один из способов получить **квантовозащищенный ключ**.

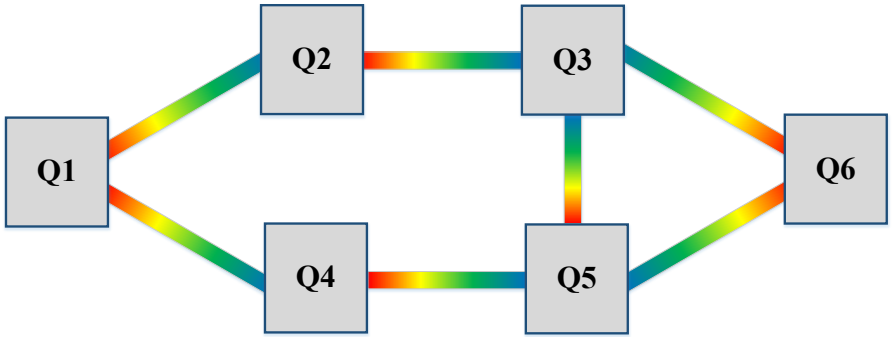
Потребители КК

- Задачи, связанные с передачей ключа конечному потребителю:
  - Работы по созданию единого защищенный интерфейса между квантовым оборудованием и СКЗИ-потребителем.
    - Обеспечение конфиденциальности и целостности команд и данных;
    - Аутентификации узлов.
  - При организации системы КРК нужно предполагать, что злоумышленник имеет меньшие возможности на канале между потребителем и квантовым оборудованием по сравнению с его возможностями на классическом аутентифицированном канале.



Построение сетей с КРК

- Криптографические задачи, возникающие при проектировании сетей с КРК:
  - Все задачи, связанные с передачей ключа конечному потребителю.
  - Задача распределения ключа между двумя несмежными узлами:
    - Выбор узлов, участвующих в распределении ключа (задача построения маршрута(-ов)).
    - Выбор способа обмена секретами.



Задача построения маршрута

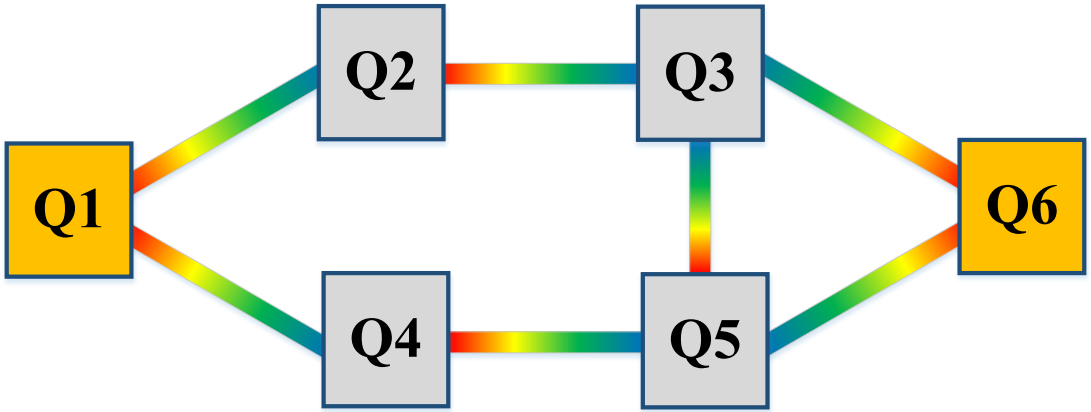


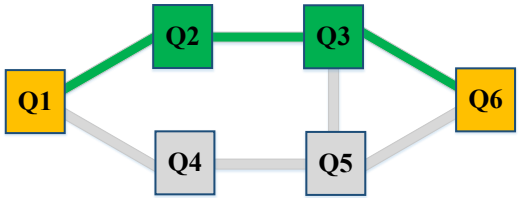
Схема квантовых связей в сети

Маршрутом от узла Q1 к узлу Q6 назовём упорядоченную последовательность узлов и каналов, которая соответствует следующим правилам:

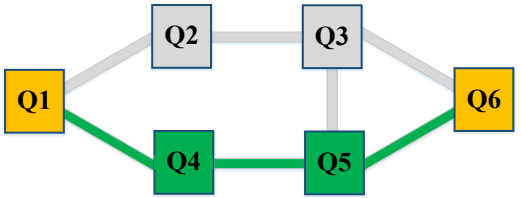
- Последовательность начинается с узла Q1 и кончается узлом Q6.
- Узлы и каналы в последовательности чередуются и не повторяются.
- Канал может стоять между двумя узлами в последовательности только в том случае, если он соединяет эти два узла.

Задача: нужно ввести метрики и строить маршруты с оптимальными метриками.

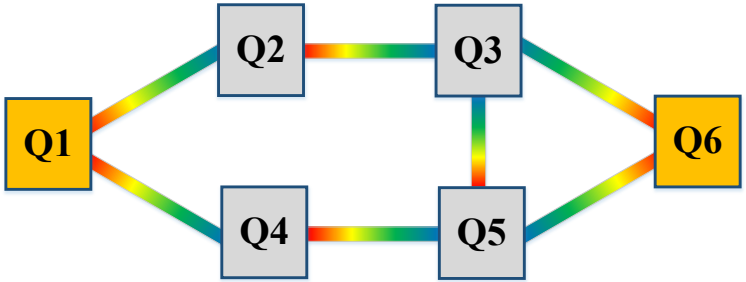
Построение маршрута



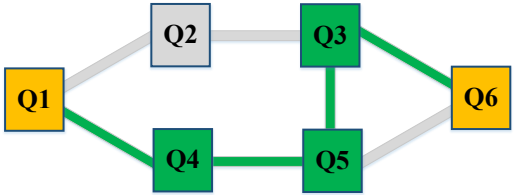
Маршрут 1



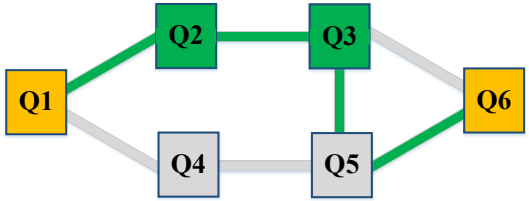
Маршрут 3



Сеть



Маршрут 2



Маршрут 4

Ключевые контейнеры

Вложенные контейнеры:

Q1:

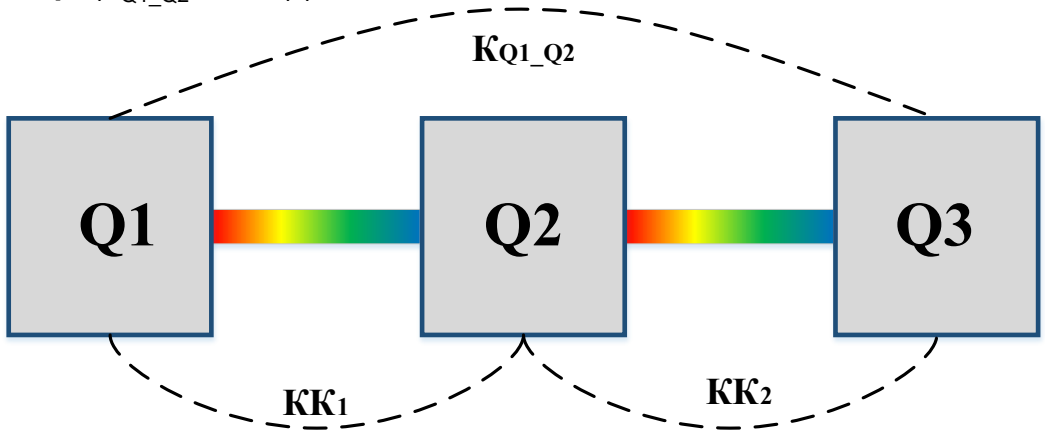
1. Создает *Ключ;*
2. Запаковывает: **Контейнер2**($КК_1$, **Контейнер1**($К_{Q1\_Q2}$, *Ключ*));
3. Отправляет Q2.

Q2:

1. «Перепаковывает»: **Контейнер2**($КК_2$, **Контейнер1**($К_{Q1\_Q2}$, *Ключ*)).
2. Отправляет Q3.

Q3:

1. Распаковывает, получает *Ключ*.



Ключевые контейнеры

Независимые контейнеры :

Q1:

1. Создает Часть_ключа_*1* *и* Часть_ключа_*2.*
2. Запаковывает: **Контейнер1**($К_{Q1\_Q2}$, Часть_ключа_*1*));
   Контейнер2($КК_1$, Часть_ключа_*2*));
3. Отправляет Q2 и Q3.

Q2:

1. «Перепаковывает»: **Контейнер2**($КК_2$, Часть_ключа_*2*));
2. Отправляет Q3.

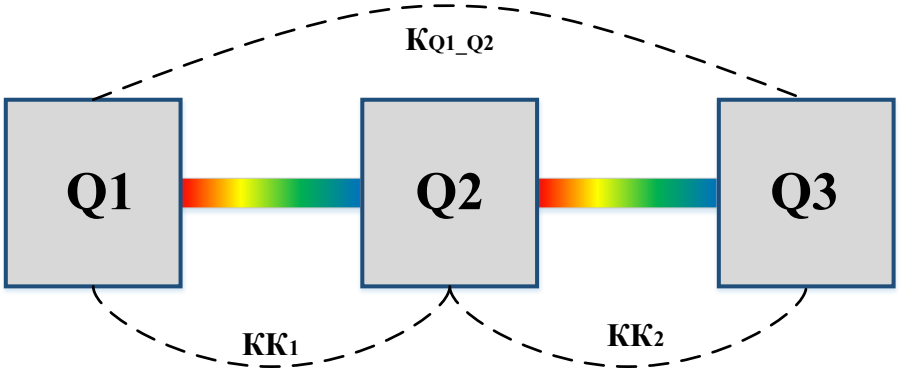
Q3:

1. Распаковывает, получает Часть_ключа_*1* *и* Часть_ключа_*2*.

Q1 и **Q3:**

Выполняют свертку и получают общий ключ:

Ключ = **Свертка**(Часть_ключа_*1,* Часть_ключа_*2, сопутствующие данные*).



infotecs

Спасибо
за внимание!