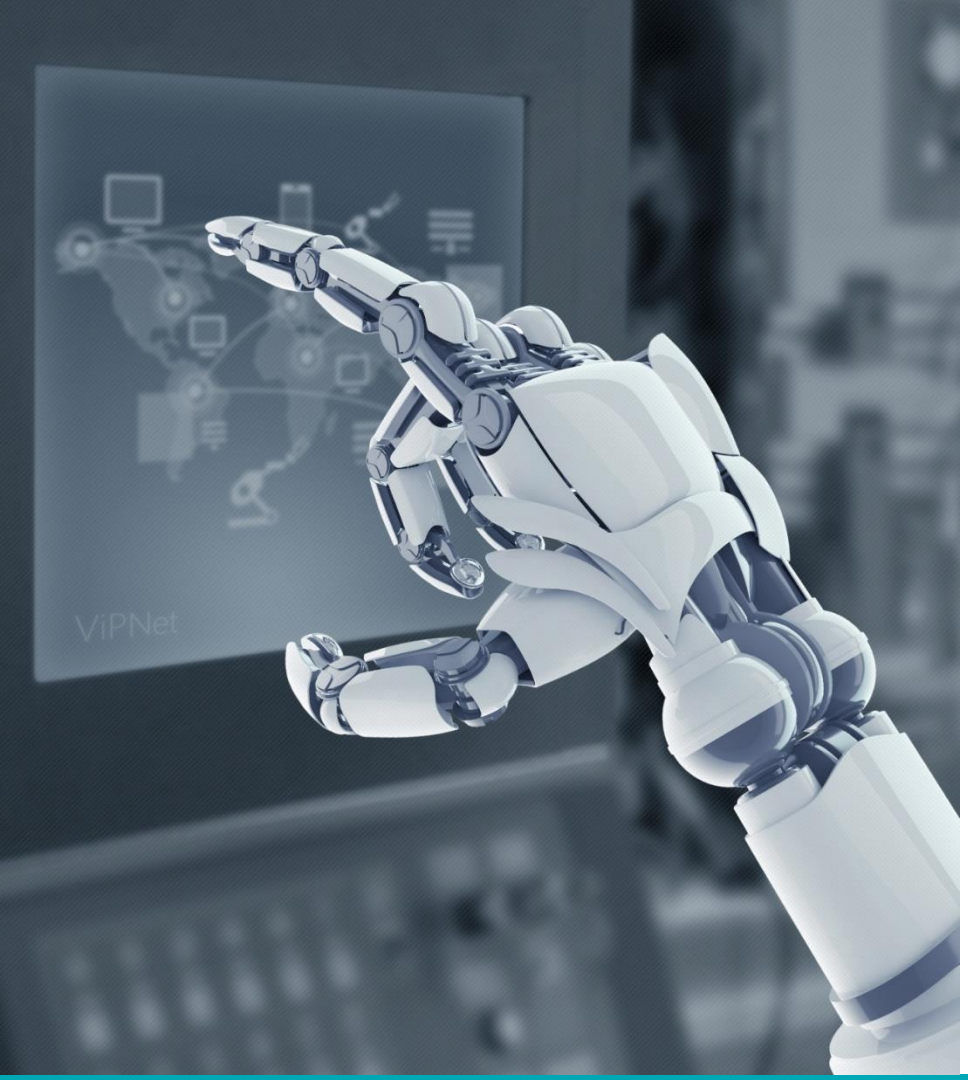
Жиляев Андрей
Старший исследователь ЦНИПР, к.т.н.

Квантовое распределение ключей



infotecs {/-cademy}

План презентации

- Введение в квантовую криптографию
- Подходы к увеличению дальности выработки квантовых ключей
- Произвольные сети квантового распределения ключей
- Квантовый маршрут и структура сети
- Проект методических рекомендаций ТК26: Ключевая система сети КРК ISTOQ-M

Введение в квантовую криптографию

Классические методы защиты

АЛГОРИТМЫ С СЕКРЕТНЫМ КЛЮЧОМ

- Защищенная передача и хранение информации
- Для взаимодействия двух участников требуется доставить обоим идентичный секретный ключ

АЛГОРИТМЫ С ОТКРЫТЫМ КЛЮЧОМ

- Для обеспечения безопасности в больших сетях
- На базе сложной математической задачи (например, факторизация)

Традиционные способы распределения секретных ключей

Доверенный курьер **доставляет ключи** из ключевого центра

Участники **вычисляют** общий ключ с использованием ассиметричных алгоритмов

Чем так страшен квантовый компьютер?

Квантовые алгоритмы для решения математических задач:

АЛГОРИТМ ШОРА → эффективное разложение числа на множители

↓

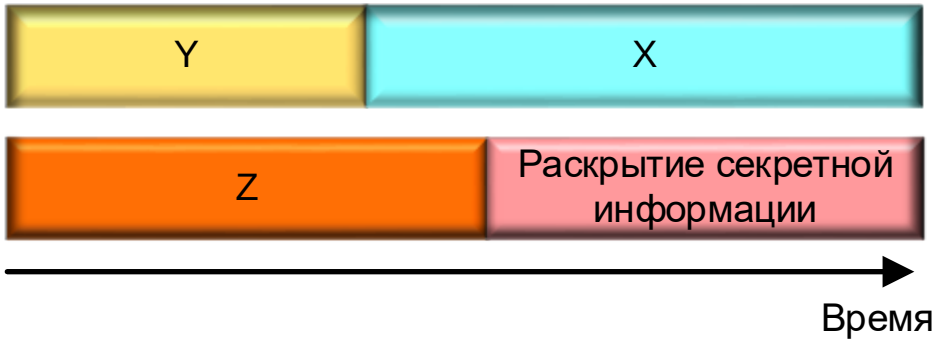
- Взломана ассиметричная криптография (протокол Диффи-Хеллмана, алгоритмы электронной подписи)

АЛГОРИТМ ГРОВЕРА → эффективный поиск по таблице (перебор)

↓

- Понижение стойкости симметричной криптографии (блочные шифры, хэш-функции)

Когда пора внедрять новые технологии?



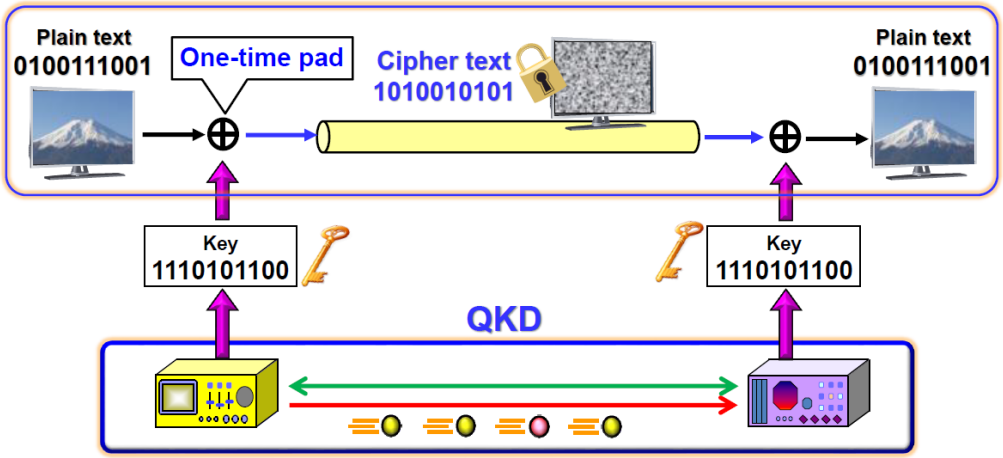
«Store Now – Decrypt Later»

X – срок актуальности информации, в течение которого информация должна оставаться защищенной

Y – время внедрения новой технологии

Z – время до появления ожидаемой угрозы

Квантовое распределение ключей



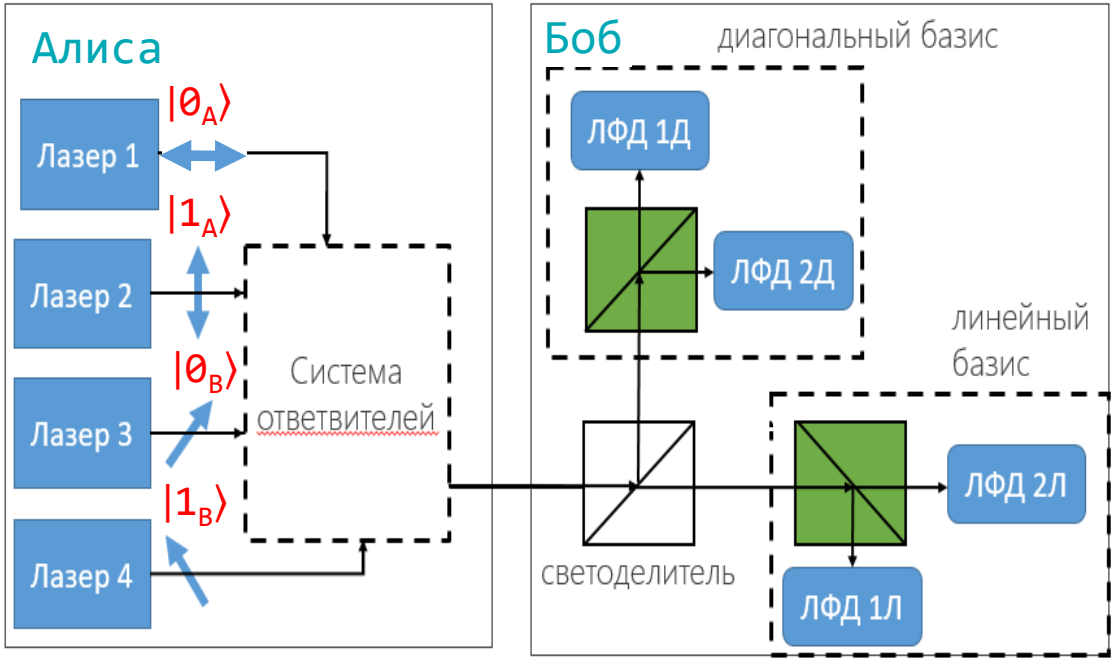
- Создание у двух абонентов общего ключа
- Способ стойкий к атакам на квантовом компьютере
- Источник ключей, обладающих теоретико-информационной стойкостью
- Доступна частая смена ключей

- Дорогие комплектующие
- Расстояние ограничено (~100км)
- Небольшая скорость создания ключей

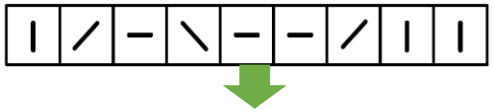
Квантовое распределение ключей

- Передача информации осуществляется с помощью квантовых состояний
- Определение совпадающих битов в независимых случайных последовательностях даёт сырой ключ
- Секретность обеспечивается за счет учёта уровня ошибок в квантовом канале
- Служебный канал криптографически аутентифицируется
- Квантовый ключ распределяется на концы квантового канала

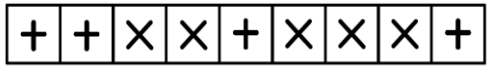
Протокол BB84. Поляризационное кодирование



Случайные состояния Алисы



Случайные базисы Боба



Случайные состояния Боба

Просеивание сырого ключа

Итоговый сырой ключ

1			1	0		0		1

Квантовое распределение ключей
Что дальше?

- Источник ключей, обладающих теоретико-информационной стойкостью
- Ограниченная дальность распределения ключей

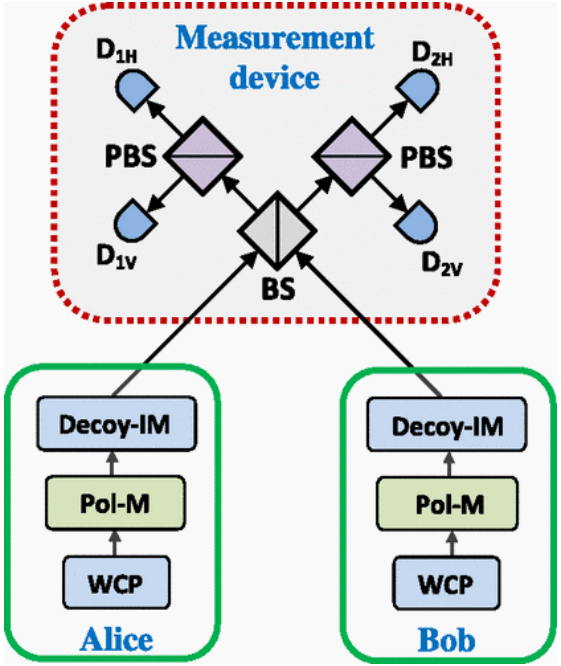
Вопрос: как покрыть большие расстояния ~ 1000 км?

Подходы к увеличению дальности выработки квантовых ключей

Специальные протоколы КРК

Measurement device independent QKD (MDI-QKD)

- Третий узел проводит сравнение полученных состояний
- Конкретные значения состояний остаются неизвестными
- Требуется когерентное излучение и синхронизация момента детектирования состояний
- Предельное расстояние ~ 300-500 км



Основные подходы к построению полносвязных сетей КРК

Квантовые повторители

- Узлы не обязаны быть доверенными
- Требуют квантовую память для передачи запутанности
- Ведутся работы по созданию
- В настоящее время как устройство не существуют
  - На их основе невозможно построить сеть КРК в настоящее время

Доверенные Узлы

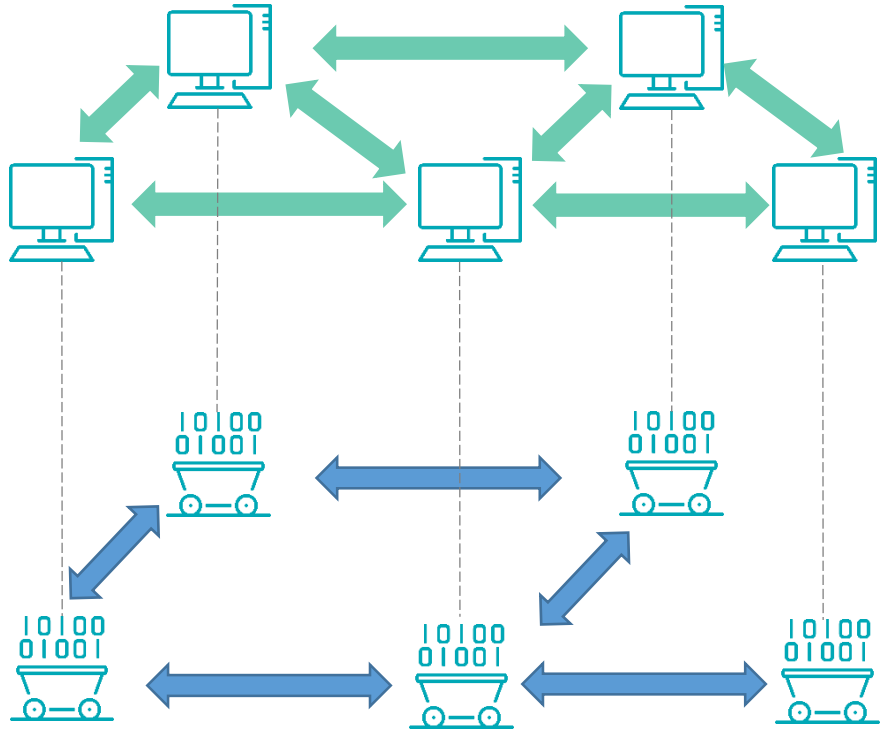
- Технологически осуществимый способ
- Критически важно доверие к узлам

Сети квантового распределения ключей

Сеть квантового распределения ключей

- Некоторые узлы сети связаны квантовыми каналами
- Сеть полносвязная на классическом уровне

- Как обеспечить секретными ключами узлы, не имеющие связей через квантовый канал?

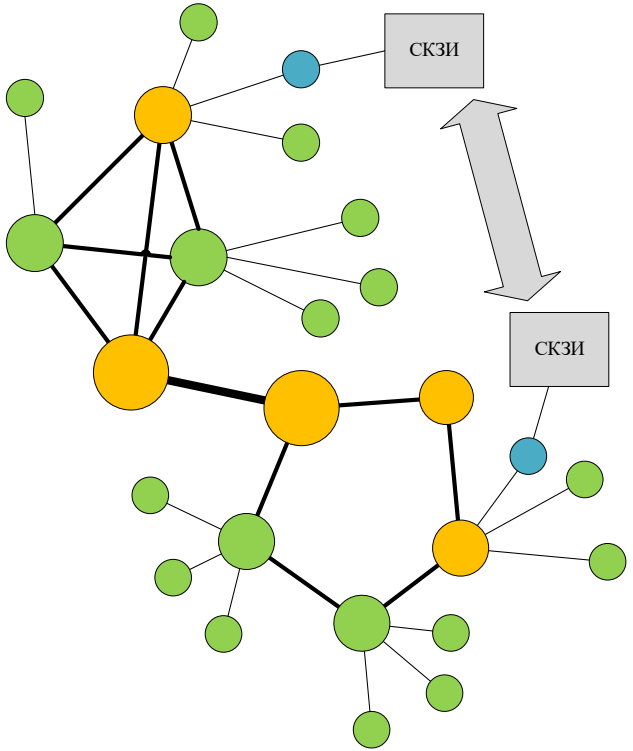


Сеть квантового распределения ключей

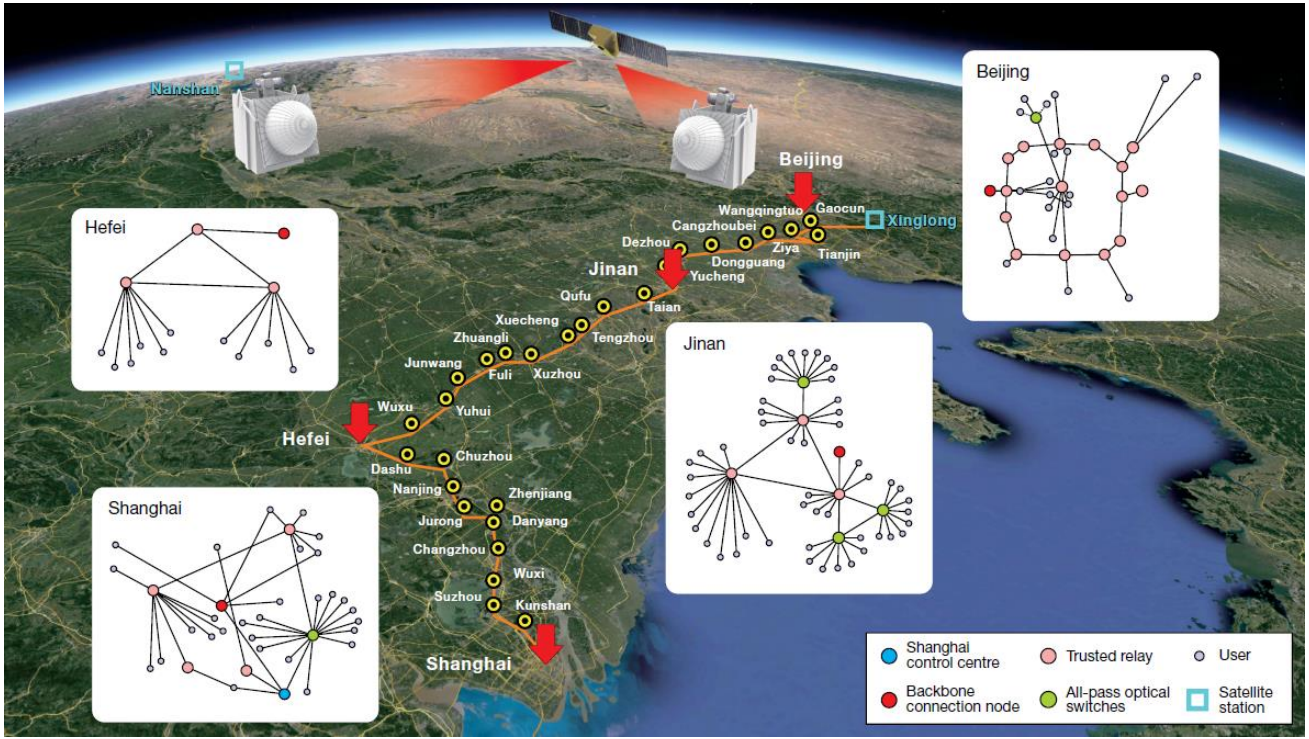
Сеть КРК основана на технологии доверенных промежуточных узлов

Каждый **узел сети (УКС)** содержит как экземпляры квантовой аппаратуры, так и служебный СКЗИ

Функция сети КРК – формирование общего секрета (целевого ключа, квантовозащищенного ключа) между любыми двумя УКС



Квантовая сеть Китая



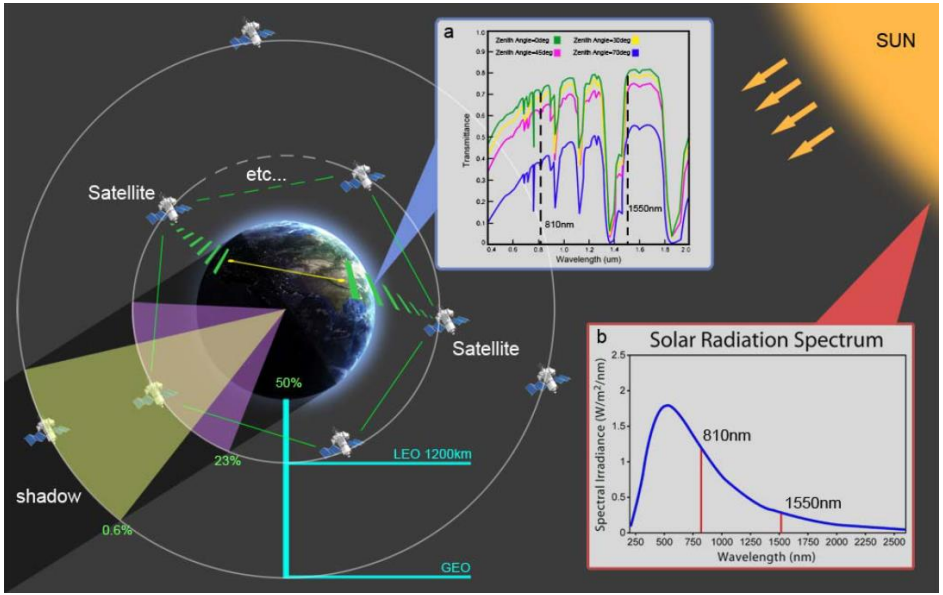
400 сегментов

2 спутника

4800 км общая протяженность

157 потребителей

Доверенные узлы в космосе



Узлы-спутники

- Меньшие потери в канале
- Малое время экспозиции
- Созвездия спутников для покрытия теневых областей земли
- Работают в паре со стационарными узлами на земле

Квантовая сеть с цепочкой доверенных узлов

- В качестве общего секрета выбирается один из квантовых ключей на сегментах сети КРК
- Конфиденциальность передачи общего секрета обеспечивается одноразовым шифроблокнотом

Недостатки:

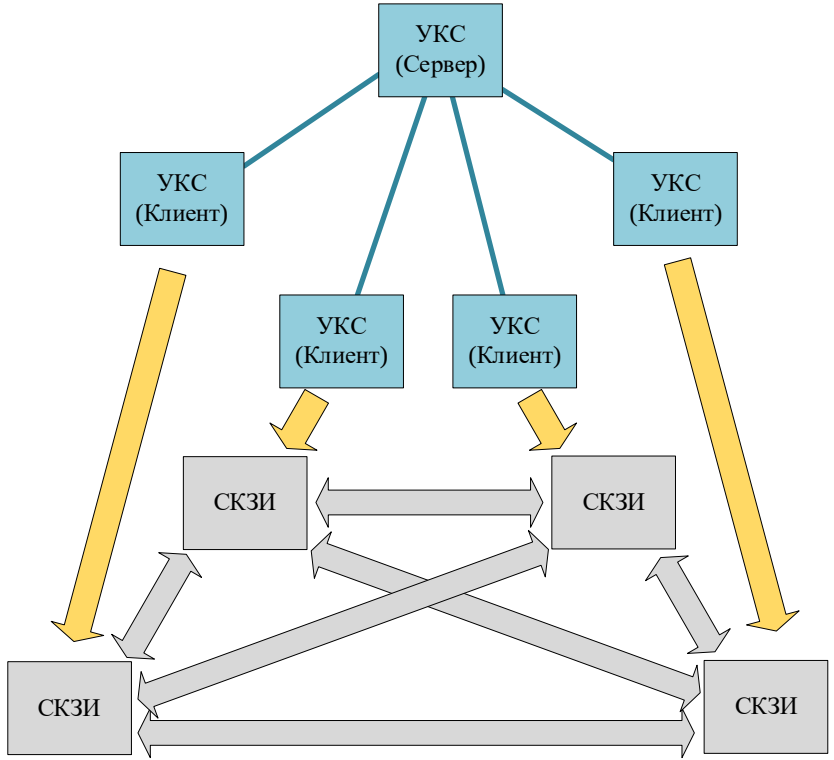
- Передаваемый секрет в открытом виде имеется на всех УКС
- Не указывается необходимость обеспечения целостности
- Нарушитель имеет некоторую информацию о квантовом ключе
  → Раскрытие информации об общем секрете

Сети КРК простых топологий

Задача: Распределить общий секрет (КЗК) между оконечными узлами сети КРК (УКС)

Звезда как магистральная линия

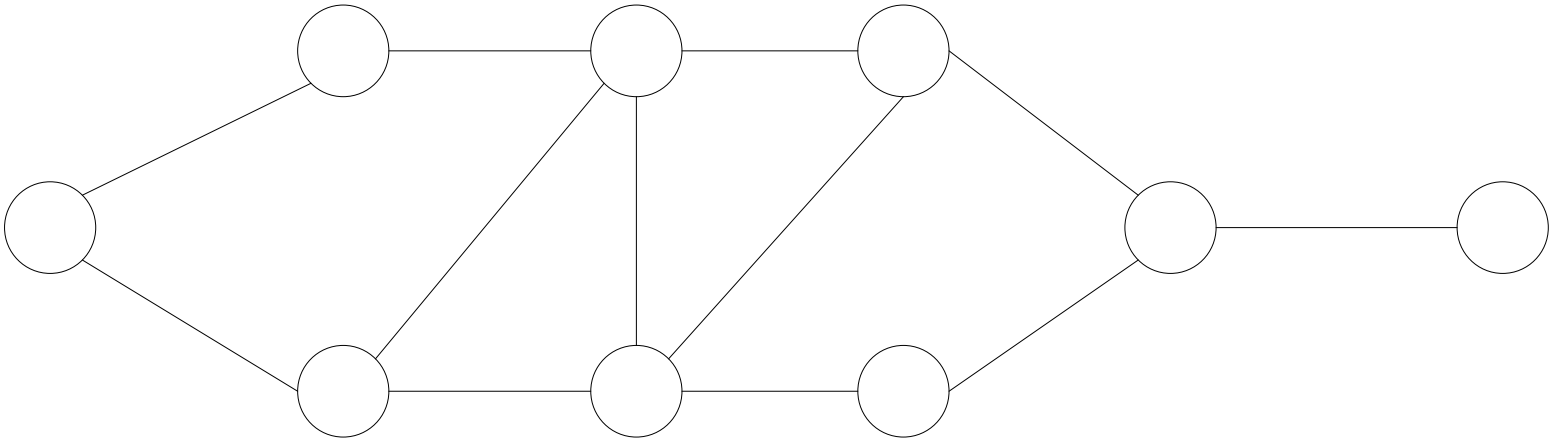
- Маршрутизация трафика – УКС Клиент → УКС Сервер → → УКС Клиент
- Сеть топологии «звезда» можно рассматривать как совокупность подсетей топологии «магистраль»
- Управление выработкой квантовых ключей удобно осуществлять из центрального УКС



Квантовый маршрут

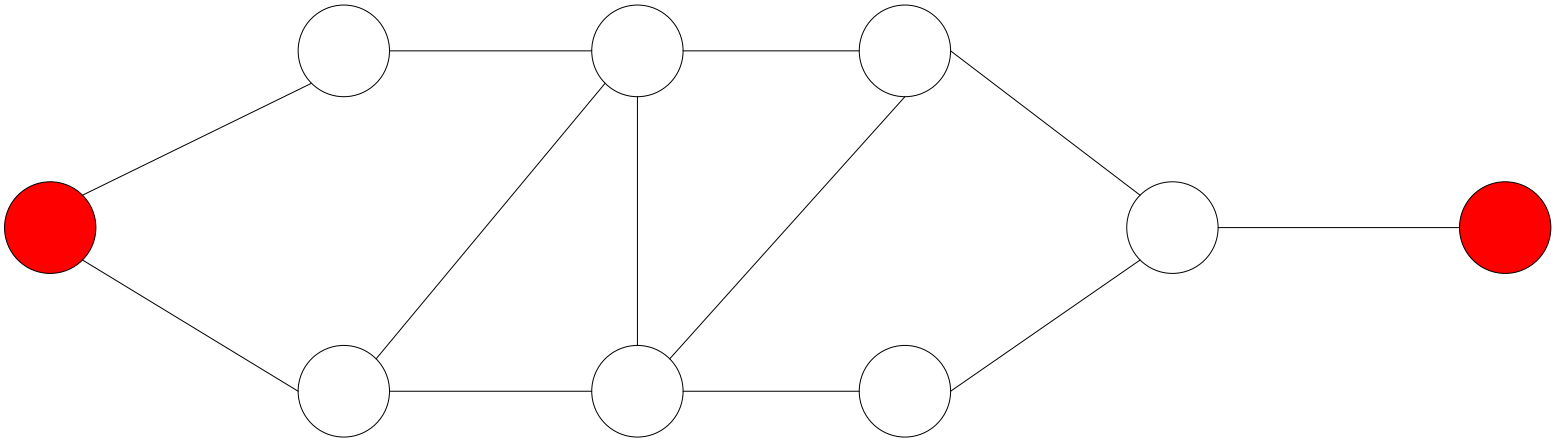
Квантовый маршрут в общем случае

Сеть КРК



Квантовый маршрут в общем случае

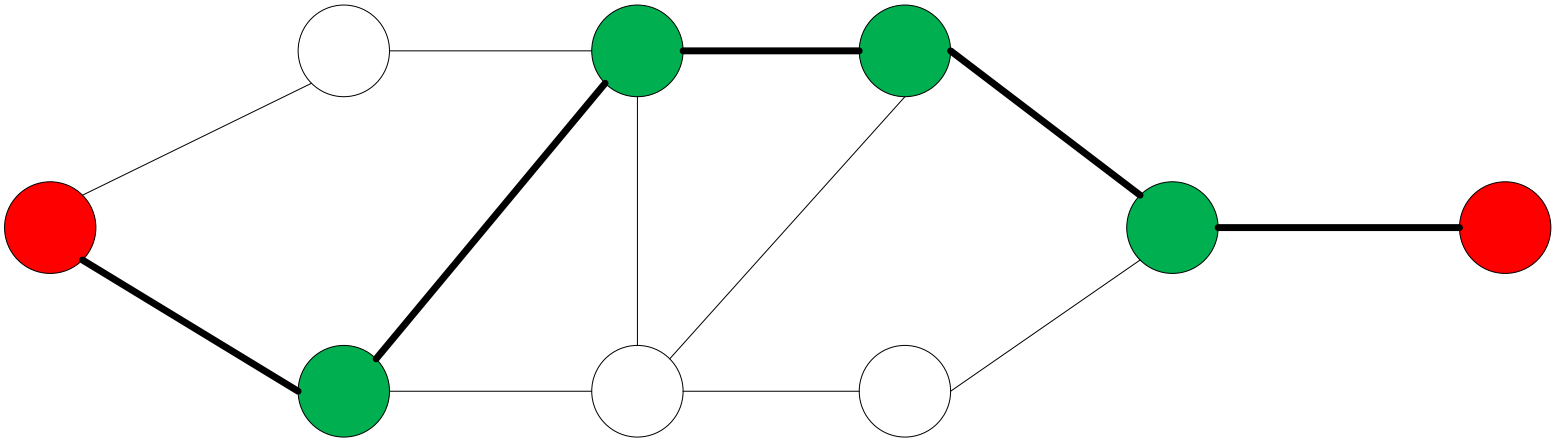
Целевые узлы



Квантовый маршрут в общем случае

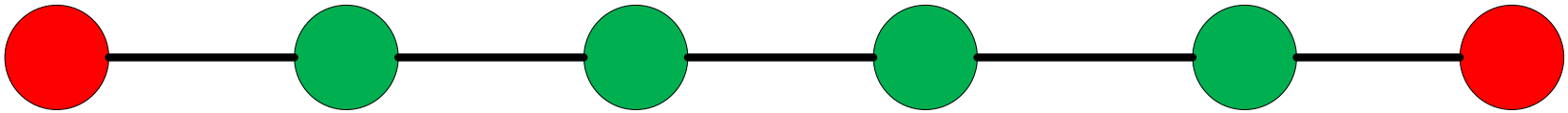
infotecs
{/-cademy}

Маршрут



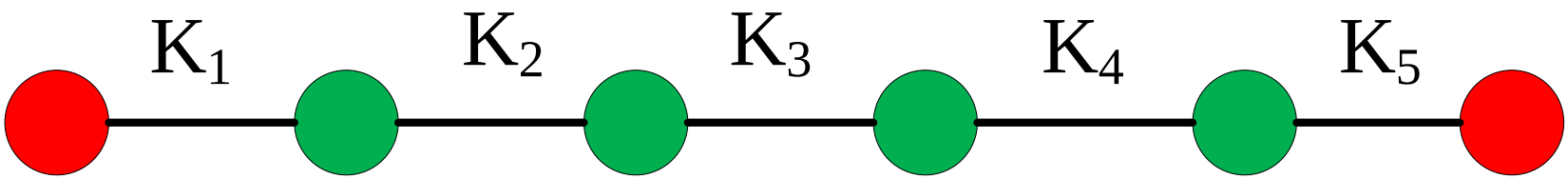
Квантовый маршрут в общем случае

Задача: выработать квантовозащищенный ключ (КЗК) между целевыми узлами



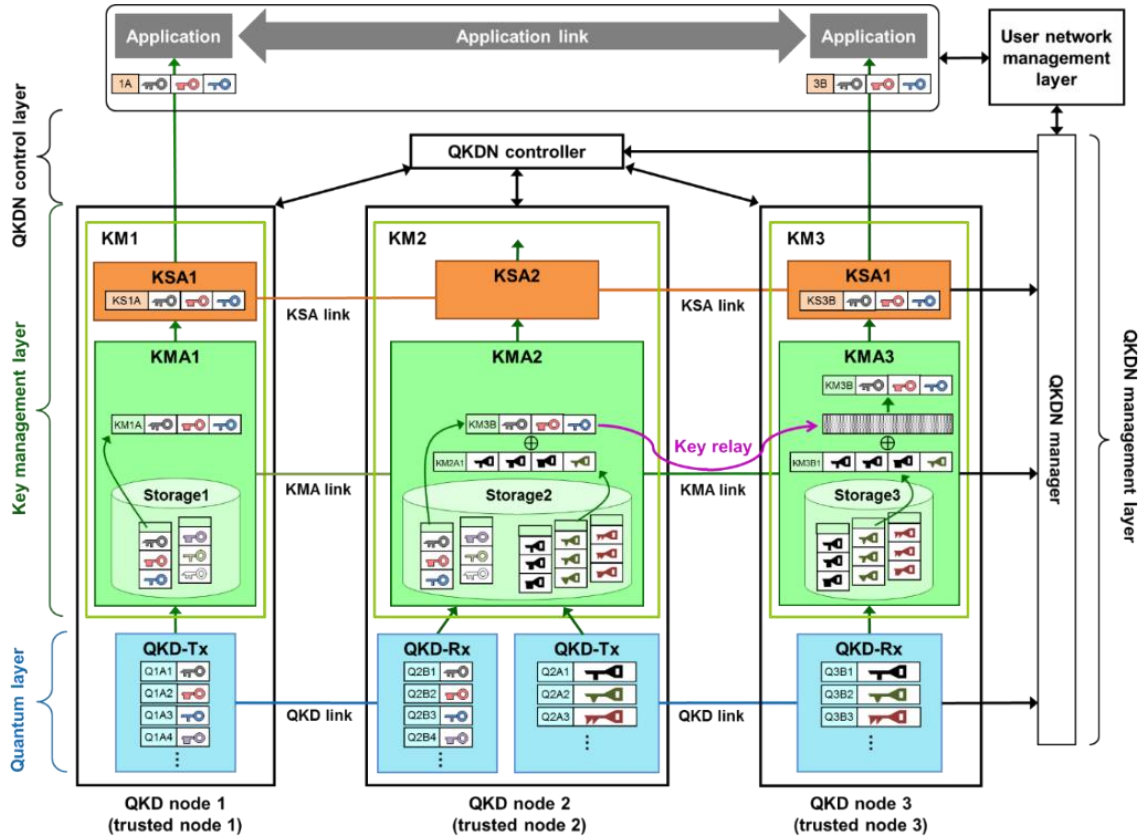
Квантовый маршрут в общем случае

Задача: выработать квантовозащищенный ключ (КЗК) между целевыми узлами

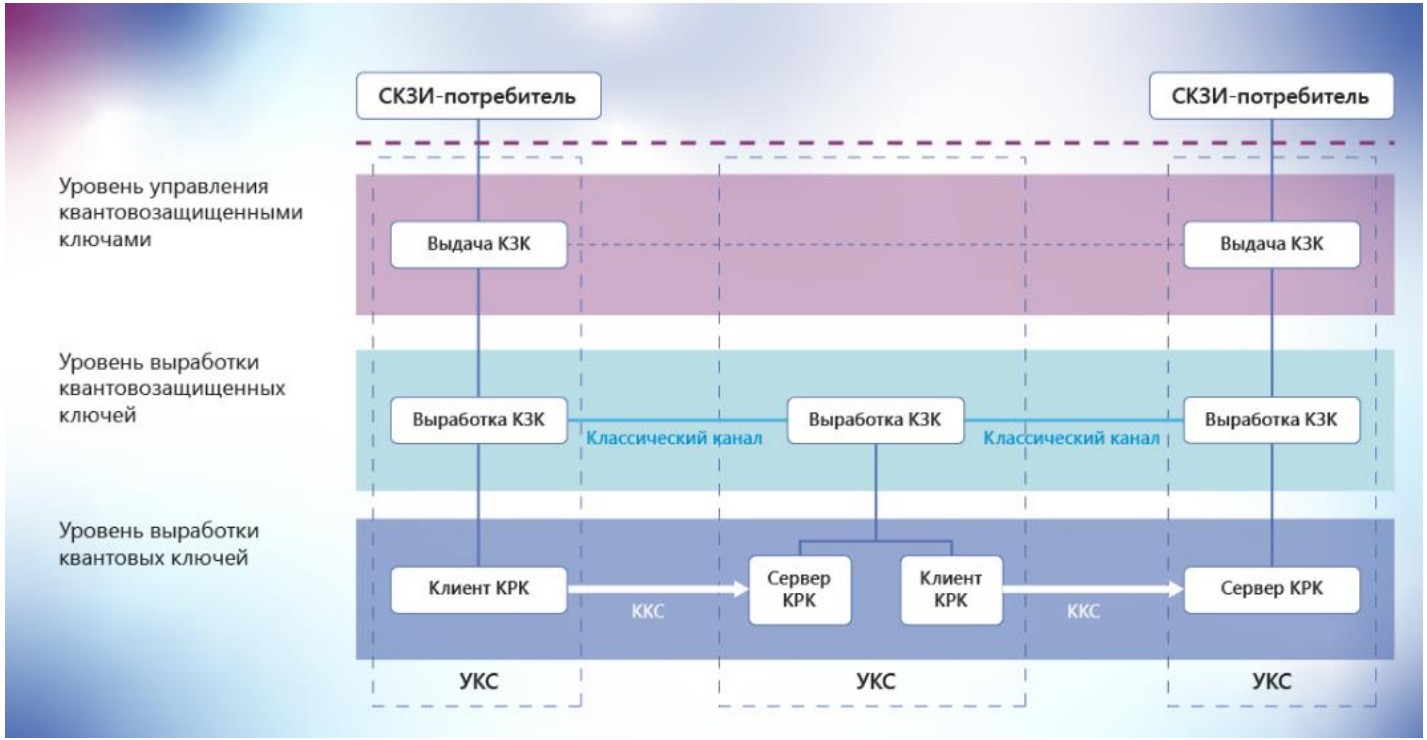


Структура сети

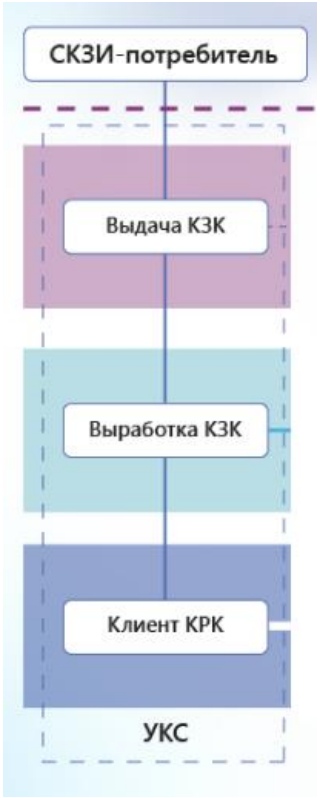
Аналоги в Европе



Наше виденье структуры сети КРК



Узел сети КРК



Модуль управления КЗК

- Организация хранилищ квантовозащищенных ключей
- Обработка запросов квантовозащищенных ключей от внешних СКЗИ

Модуль выработки КЗК

- Поддержание актуальной карты сети
- Построение оптимального маршрута по распределению квантовозащищенных ключей
- Распределение квантовозащищенных ключей
- Организация хранилищ квантовых ключей
- Управление выработкой квантовых ключей

Модуль выработки КК

- Выработка квантовых ключей

Требуемые функции уровней сети КРК

Уровень **потребителей:**

- запрос квантовозащищенного ключа (с указанием желаемых или требуемых параметров);
- получение КЗК согласно запросу;
- использование ключа согласно предписанию в устройствах этого уровня.

Уровень **управления КЗК:**

- организация хранилищ квантовозащищенных ключей;
- синхронизация ключевых хранилищ попарно (по наличию связи);
- мониторинг запросов на квантовозащищенные ключи (прогнозирование);
- обработка запросов квантовозащищенных ключей от внешних СКЗИ;
- формирование запросов квантовозащищенных ключей к нижестоящему уровню выработки квантовозащищенных ключей;
- получение квантовозащищенных ключей от уровня выработки квантовозащищенных ключей;
- передача квантовозащищенных ключей СКЗИ-потребителю.

Требуемые функции уровней сети КРК

Уровень **выработки КЗК:**

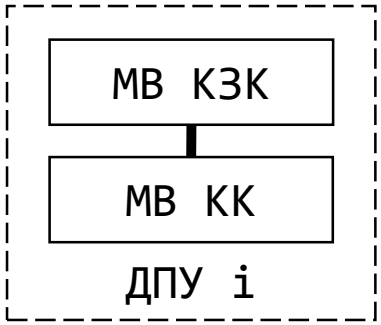
- поддержание актуальной карты сети;
- построение оптимальных цепочек УКС для формирования КЗК;
- распределение КЗК на определенных цепочках УКС;
- организация хранилищ квантовых ключей;
- организация каналов, защищенных на квантовых ключах (для формирования КЗК);
- организация запросов квантовых ключей;
- передача квантовозащищенных ключей на уровень управления квантовозащищенными ключами в ответ на запрос таких ключей.

Уровень **выработки квантовых ключей:**

- выработка квантовых ключей;
- передача квантовых ключей на уровень выработки квантовозащищенных ключей.

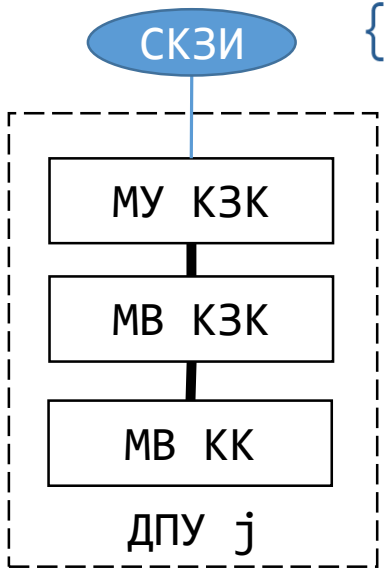
Ключевая система сети КРК ISTOQ-M

Логическая структура ДПУ



ДПУ без СКЗИ-потребителя

- МВ КК – создание квантовых ключей (КК)
- МВ КЗК – создание квантовозащищенных ключей (КЗК)

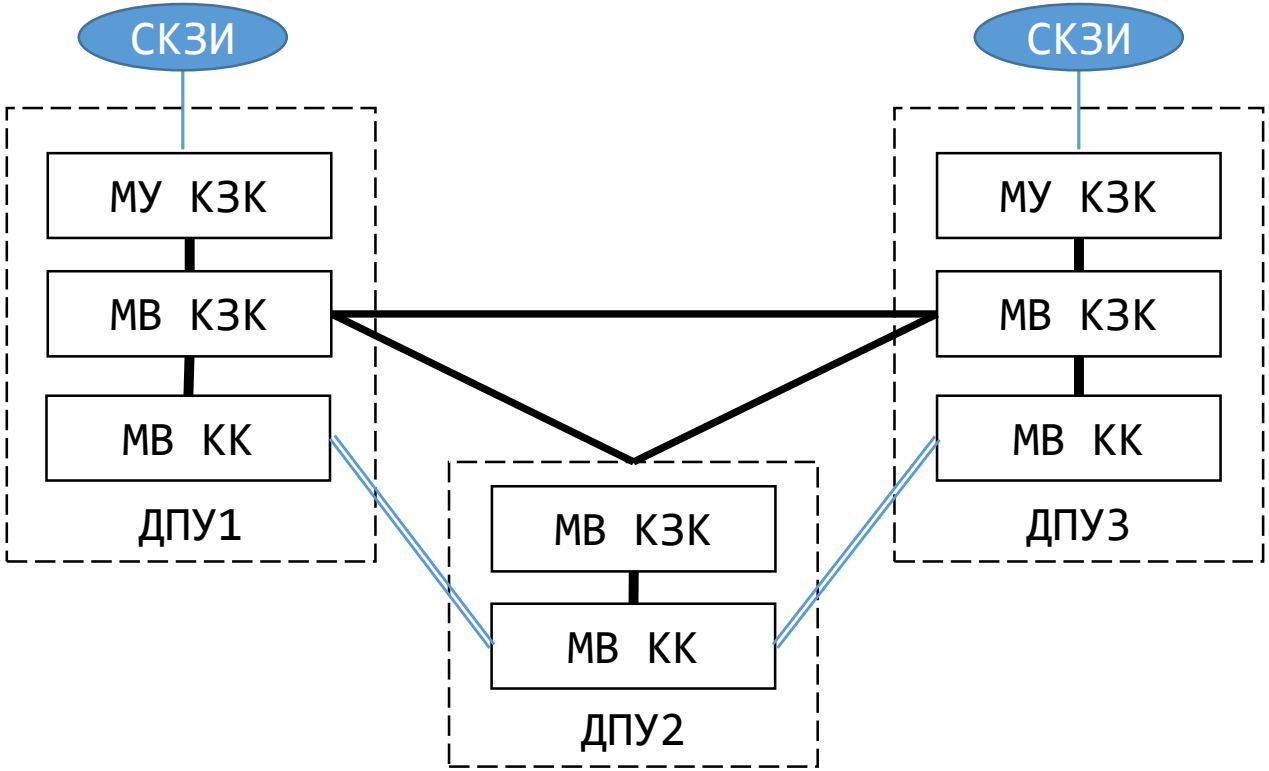


ДПУ с СКЗИ-потребителем

Дополнительно:

- МУ КЗК – взаимодействие с СКЗИ-потребителем

Сеть на базе ДПУ - Архитектура



ДПУ1 – ДПУ3:
сопряженные, целевые

ДПУ1 – ДПУ2:
сопряженные, соседние

ДПУ2 – ДПУ3:
сопряженные, соседние

классический канал

квантовый канал

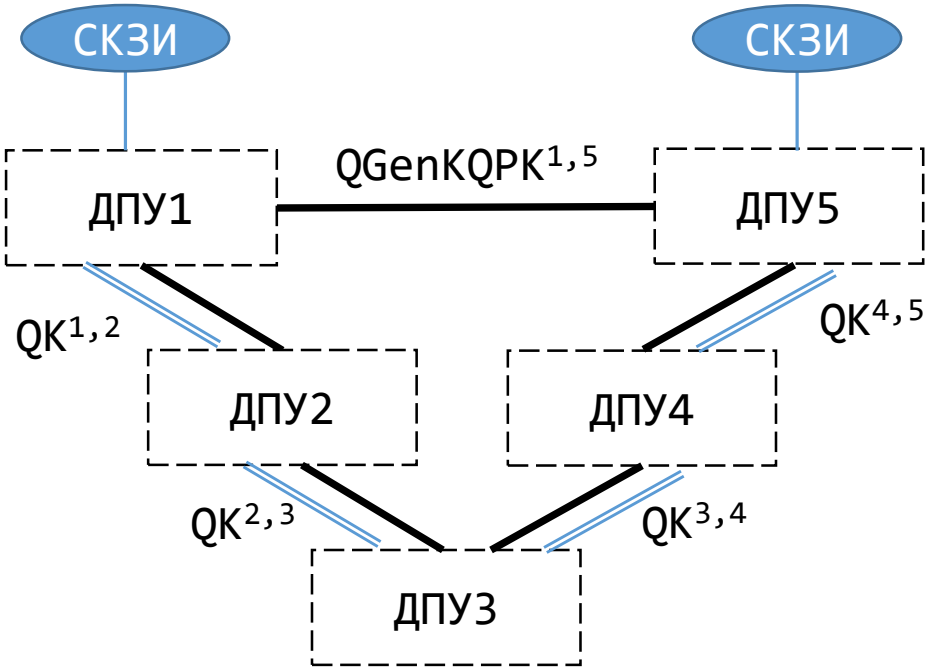
Ограничения/требования для ключевой системы

- ДПУ поименованы
- ДПУ знают друг о друге
- ДПУ умеют построить маршрут для выработки КЗК
- Граф связей квантовыми каналами связный
- Структура ДПУ может различаться:
  - Единое устройство
  - Набор устройств
  - Прочие варианты

Протокол выработки общего ключа Требования

- Общий ключ (КЗК) создается для любой пары целевых ДПУ
- КЗК гибридный – создан с использованием квантовой и классической ключевой подсистемы
  - Компрометация одной из подсистем не приводит к компрометации КЗК
- Протокол масштабируем на сети произвольной топологии с произвольным числом ДПУ

Протокол выработки общего ключа
Предусловия



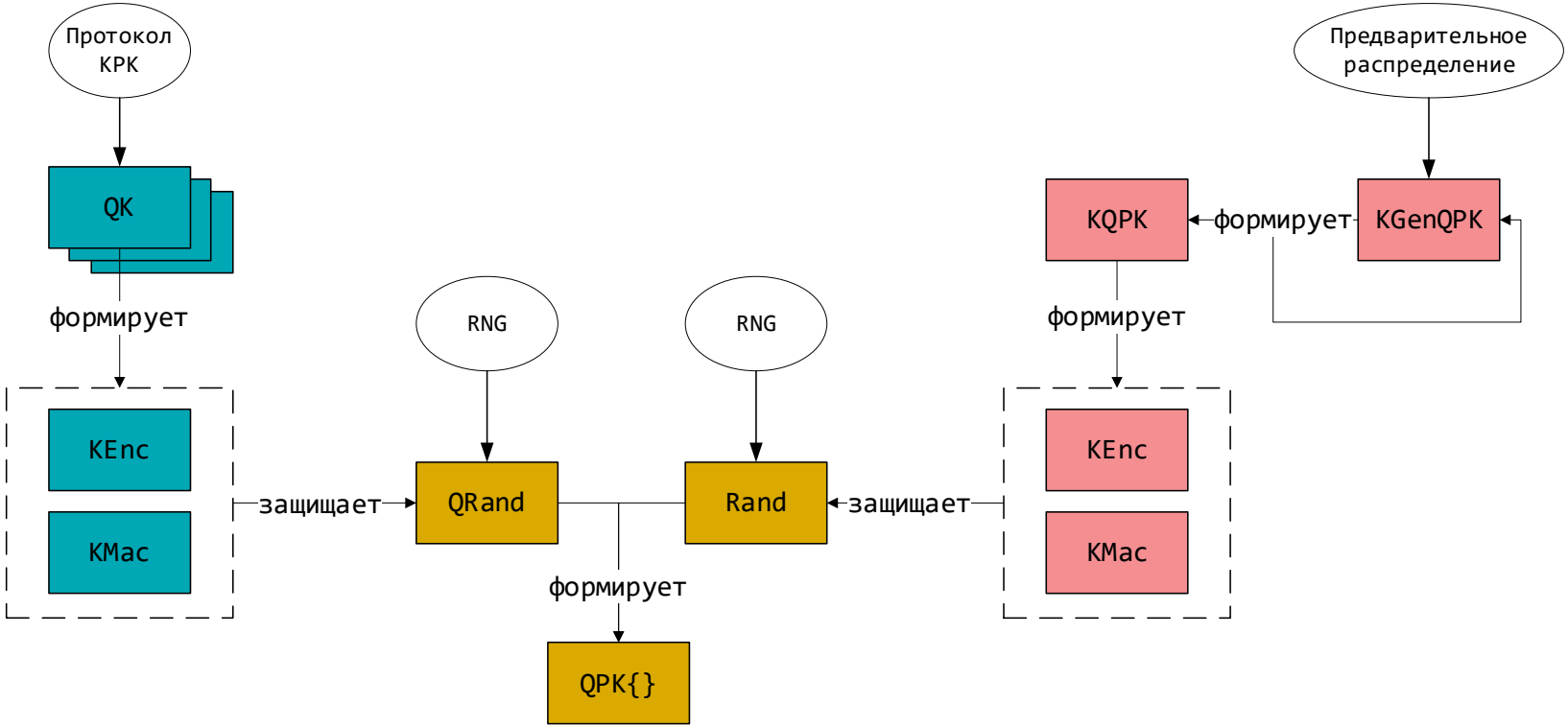
Созданы:

- $QK^{1,2}$, $QK^{2,3}$, $QK^{3,4}$, $QK^{4,5}$, – квантовые ключ

Загружен

- $QGenKQPK^{1,5}$ – ключ генерации ключей защиты КЗК (для классической составляющей)
  - Служит для создания ключей KQPK

Рассматриваемые множества ключей



Протокол выработки общего ключа
Принципы

- КЗК создается из компонент Rand и QRand
- Каждая компонента суть ключевая информация
- Часть компонент передается с защитой на классических ключах (выводятся из KGenKQPK классическими методами) – классические компоненты Rand
- Часть компонент передается с защитой на квантовых ключах QK – квантовые компоненты Qrand
- Компрометация или классических ключей, или квантовых ключей не приведет к компрометации КЗК

Протокол выработки общего ключа Криптографические алгоритмы

infotecs {/-cademy}

- Вывод ключей защиты составляющей КЗК Rand

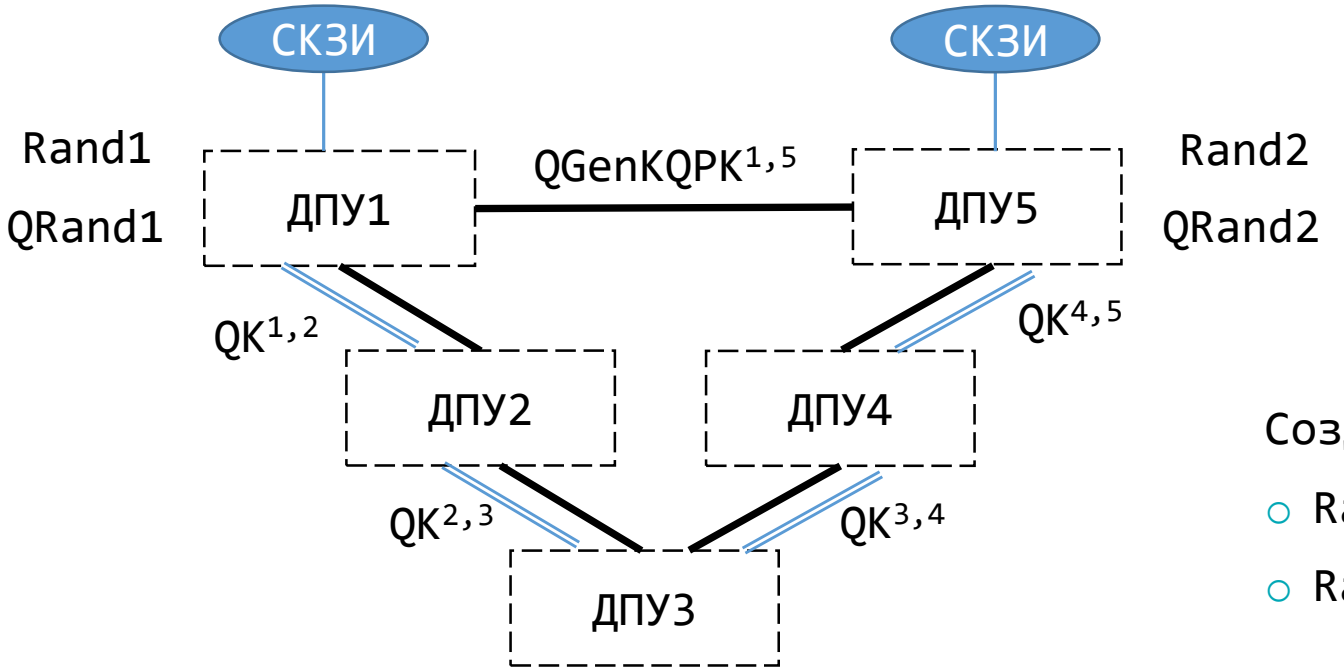
$$\boldsymbol{KDF1}\left(KGenQPK_j^{t,p}\right) = \mathrm{KDF}_{\mathrm{TREE\ 256}}\left(\mathrm{K}GenQPK_j^{t,p}, \mathrm{label}, \mathrm{seed}, 1\right) = =$$
$$KQPK_j^{t,p} || KQPK_j^{p,t} || KgenQPK_{j+1}^{t,p}$$
$$seed = Counter_{K_i},\ label = const$$

- Функция гибридизации

$$\boldsymbol{KDFG}\left(Rand_n^{t,p}, Rand_n^{p,t}, QRand_n^{t,p}, QRand_n^{p,t}\right) = KDF(S, L, T, P, U, A) =$$
$$= QPK_n^{t,p} = \left\{QPK_n^{(1)\,t,p}, QPK_n^{(2)\,t,p}, \ldots, QPK_n^{(M)\,t,p}\right\}$$

- Ключевые контейнеры:
  - CS_KW = 0 - KExp15-KImp15-Kuzn;
  - CS_KW = 1 - KExp15-KImp15-Magma.

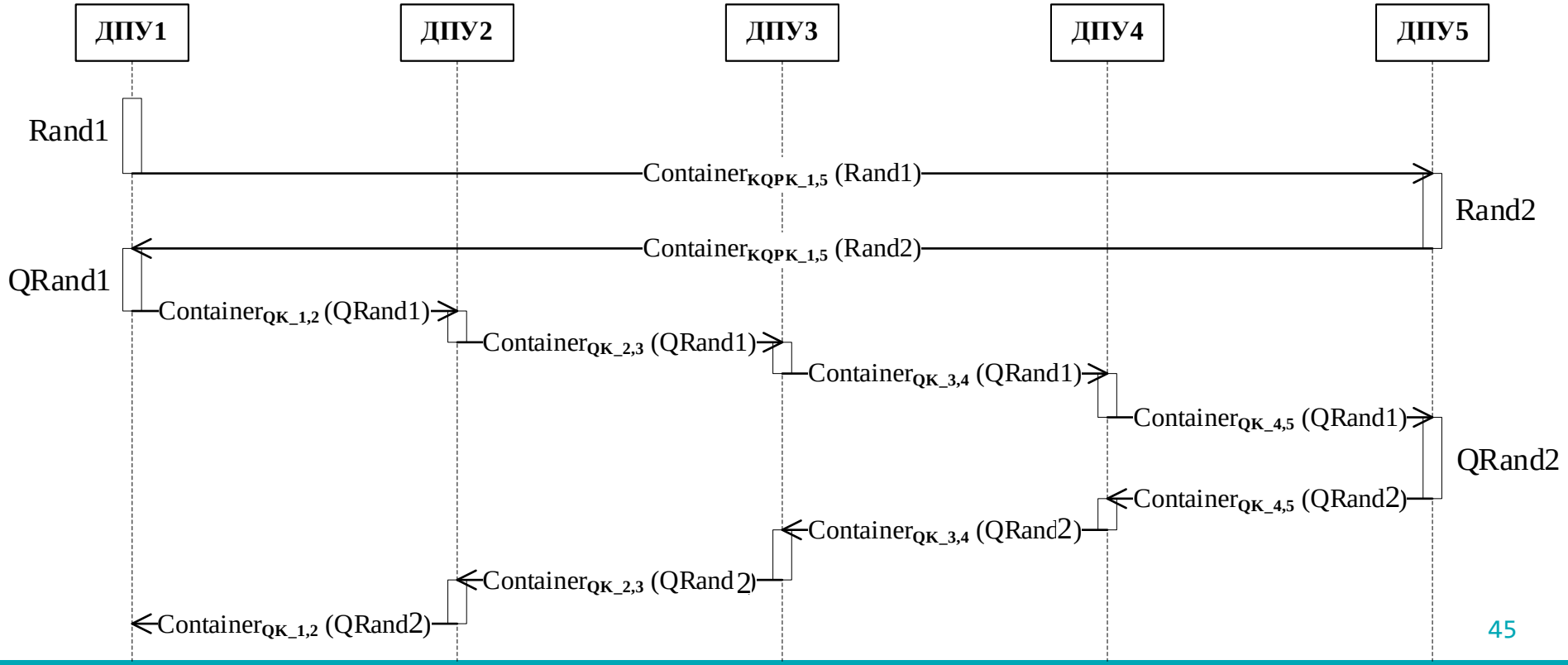
Протокол выработки общего ключа
Создание компонент



Созданы:

- Rand1, QRand1
- Rand2, QRand2

Протокол выработки общего ключа
Передача компонент



Протокол выработки общего ключа
Формат контейнера

infotecs {/-cademy}

$$\boldsymbol{Container} = label \| n \| CS\_KW \| ID_{K_i} \| Counter_{K_i} \| Node_p \| Node_t \| Node_a \| Node_b \| KEXP$$

$\boldsymbol{label} \in V_{64}$ – метка, обозначающая тип используемого ключа. $label$ = ‘QK’ = 0x00000000514b. $label$ = ‘KQPK’ = 0x00004b51504b;

$\boldsymbol{n} \in V_{128}$ – идентификатор набора КЗК, для которого передается составляющая. Способ формирования идентификатора должен быть согласован всеми участниками информационного обмена;

$\boldsymbol{ID_{K_i}} \in V_{128}$ – идентификатор ключа для формирования экспортного представления;

$\boldsymbol{Counter_{K_i}}$ – счетчик использования ключа, используемый в качестве IV;

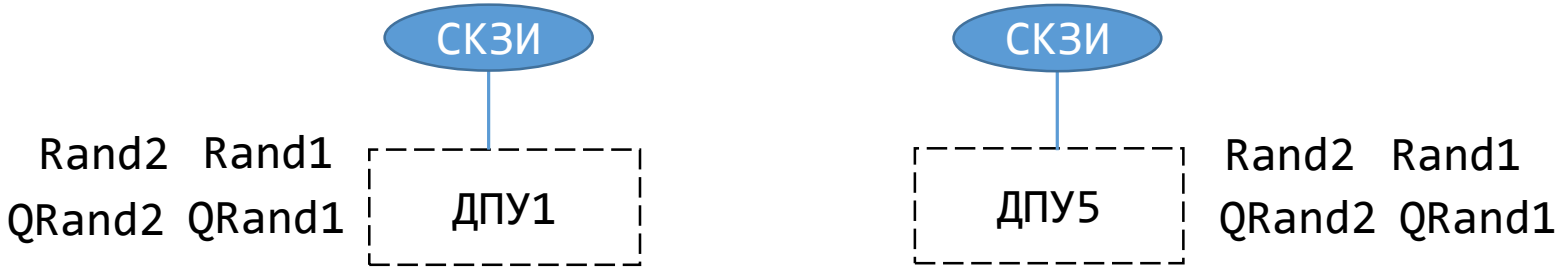
$\boldsymbol{Node_a} \in V_{128}$, $\boldsymbol{Node_b} \in V_{128}$ – идентификаторы узлов, на котором и для которого создан ключевой контейнер;

$\boldsymbol{Node_p} \in V_{128}$, $\boldsymbol{Node_t} \in V_{128}$ – идентификатор узлов, на котором и для которого создана передаваемая составляющая;

$\boldsymbol{CS\_KW} \in V_8$ – используемый криптонабор для экспортного представления составляющей КЗК;

$\boldsymbol{KEXP}$ – экспортное представление передаваемой составляющей КЗК;

Протокол выработки общего ключа Создание КЗК



Составляющие Rand1, Rand2, QRand1, QRand2 на каждом ДПУ смешиваются с помощью функции гибридизации KDFG()

- KDFG построена на базе Р 1323565.1.022-2018 Информационная технология. Криптографическая защита информации. Функции выработки производного ключа
- Функция KDFG создает **набор КЗК (**несколько КЗК из одного комплекта составляющих)

Протокол выработки общего ключа Свойства

- Симметричный – два целевых ДПУ в равной степени участвуют в протоколе
- КЗК гибридный – компрометация одной ключевой подсистемы не компрометирует КЗК
- Масштабируемый – если квантовая сеть связная, то последовательность соседних ДПУ, соединяющая два целевых ДПУ существует => существуют требуемые квантовые ключи
- Допустимо использование только компонент QRand => Составляющие КЗК Rand фиксированы

Функция гибридизации KDFG ()

$$KDFG\left(Rand_m^{t,p}, Rand_m^{p,t}, QRand_m^{t,p}, QRand_m^{p,t}\right) = KDF(S, L, T, P, U, A)$$
$$= QPK_m^{t,p} = \left\{QPK_m^{(1)\,t,p}, QPK_m^{(2)\,t,p}, \dots, QPK_m^{(M)\,t,p}\right\},$$

- $S \in V_{256}$ – исходная ключевая информация. $S = HASH_{256}\left(QRand_m^{t,p} || QRand_m^{p,t}\right)$;
- $L \in V_{32}$ – суммарная длина целевых ключей формируемого набора КЗК;
- $T \in V_{256}$ – соль. $T = HASH_{256}\left(Rand_m^{t,p} || Rand_m^{p,t}\right)$;
- $P \in V_{64}$ – метка использования, назначение ключа – КЗК(QPK);
- $U \in V_{256}$ – идентификаторы пары ДПУ. $U = Node_t || Node_p$;
- A – дополнительная информация, идентификатор набора КЗК m.

Функция гибридизации KDFG ()

На первом этапе вычисляется промежуточный ключ:

$$K^{(1)} = S \oplus T,$$

На втором этапе из промежуточного ключа создается выходная последовательность длины L: $Z = z_1||z_2||\ldots||z_{2M}$,

Где: $z_l = CMAC_{K^{(1)}}\left(m||C_l||P||U||L\right)$,

- $C_l \in V_{16}$ – битовое представление номера блока l длиной 16 бит;
- $m \in V_{48}$ – идентификатор формируемого набора ЦК.

Выходная последовательность Z разбивается на блоки длины 256 бит. Каждый блок длины 256 бит является ЦК из формируемого набора ЦК.

$$QPK_m^{(j)} = z_{2j-1}||z_{2j}$$

Вопросы?

infotecs
{/-cademy}

Спасибо за внимание!

Жиляев Андрей
Старший исследователь ЦНИПР

Подписывайтесь на наш канал

infotecs {/-cademy}