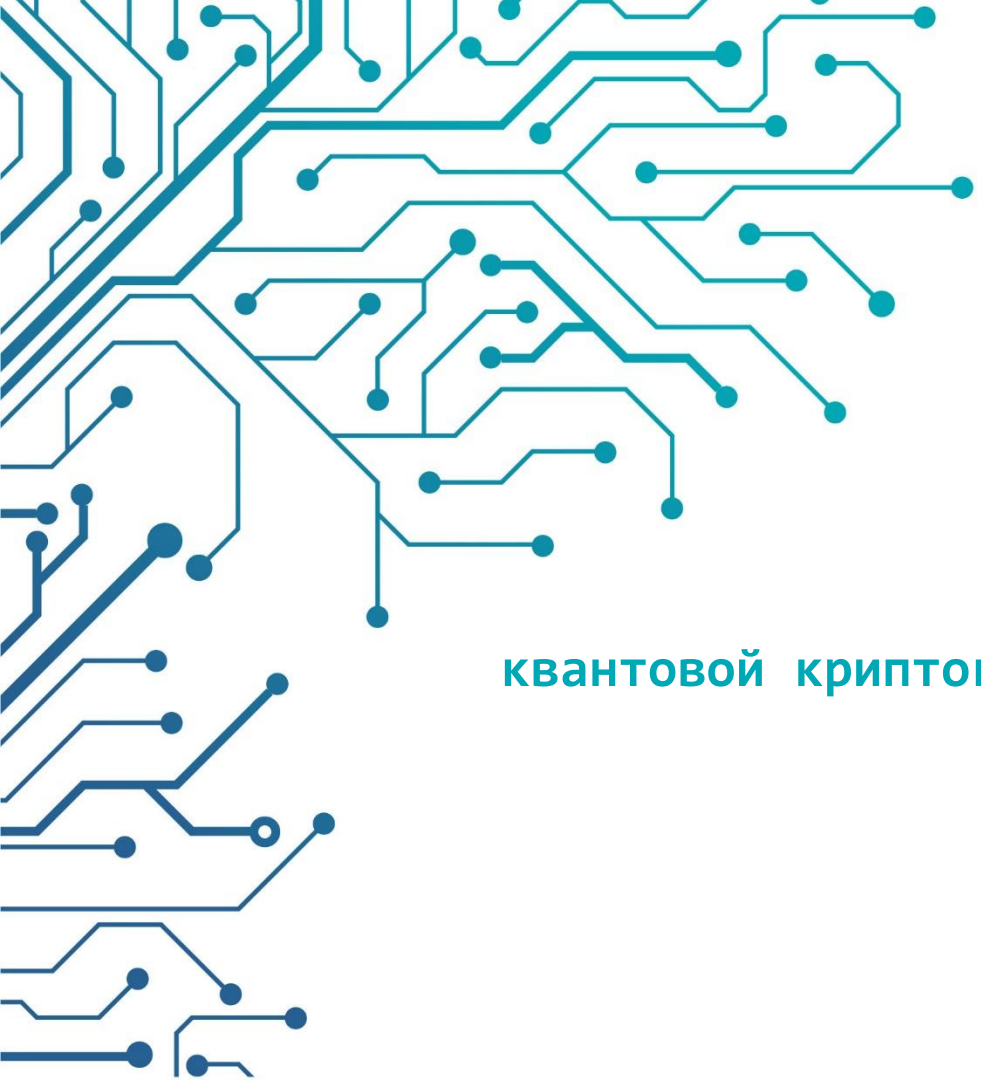
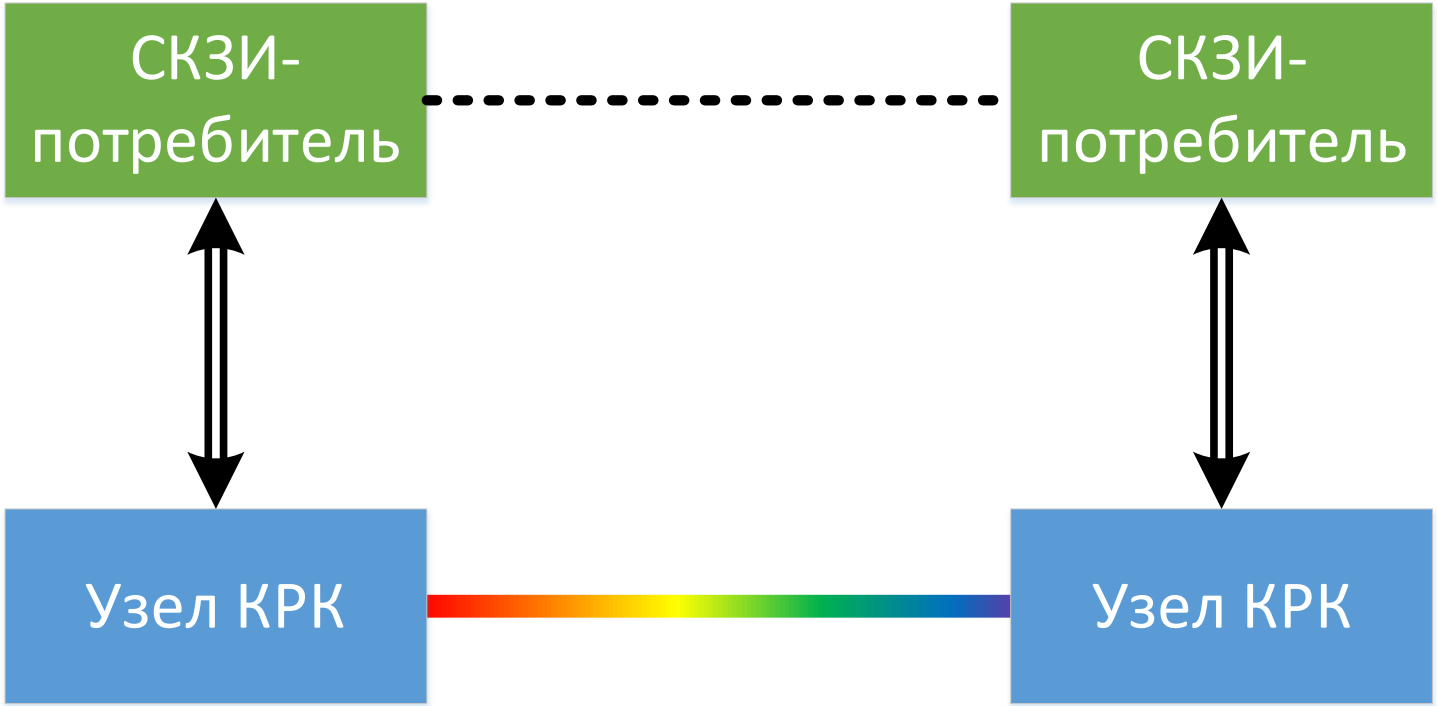


О стандартизации механизмов квантовой криптографии в РФ. ProtoQa и IstoQ

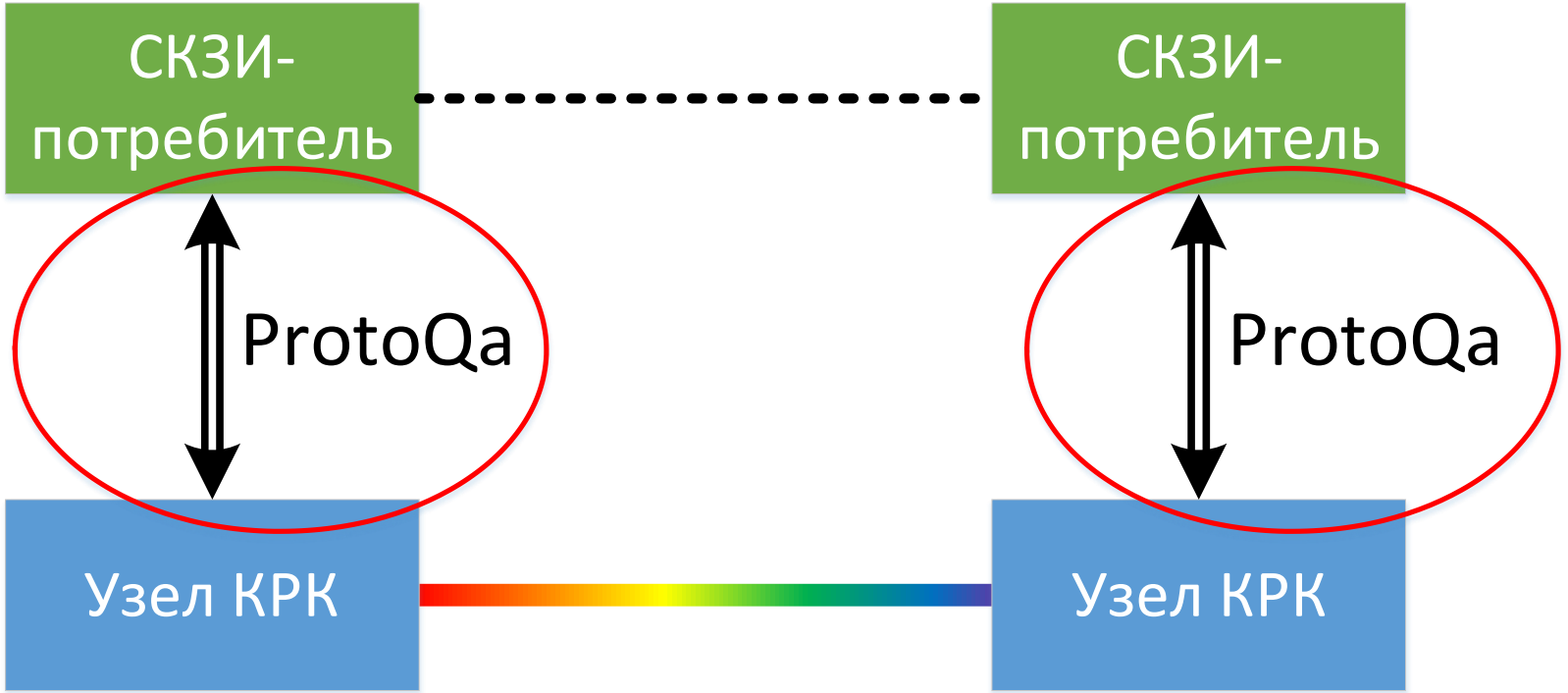
Науменко Антон Павлович, ООО СФБ Лаб
Бородин Михаил Алексеевич, АО Инфотекс
Жиляев Андрей Евгеньевич, АО Инфотекс

Защищенный протокол взаимодействия ККС ВРК и СКЗИ(ProtoQa)

Введение



Введение


СКЗИ-потребитель
СКЗИ-потребитель
ProtoQa
ProtoQa
Узел КРК
Узел КРК

Задача протокола ProtoQa

Главной задачей протокола «Протока» является обеспечение защищенного взаимодействия между узлом квантовой сети и потребителем ключей. Протокол построен по принципу запрос-ответ.

Структурные особенности ProtoQa

Конфиденциальность и имитозащита передаваемых данных, а также защита от навязывания ранее переданных сообщений обеспечивается использованием протокола CRISP.

В составе криптографически защищенных сообщений между узлом КРК и СКЗИ-потребителем Протока может передавать криптографические ключи, случайные числа и сервисную информацию.

Защита ключевого материала при передаче

При передаче ключей между узлом КРК и СКЗИ-потребителем в сообщении для дополнительной защиты формируется экспортное представление ключа – ключ передается внутри криптографически защищенного ключевого контейнера, сформированного по алгоритму KExp15

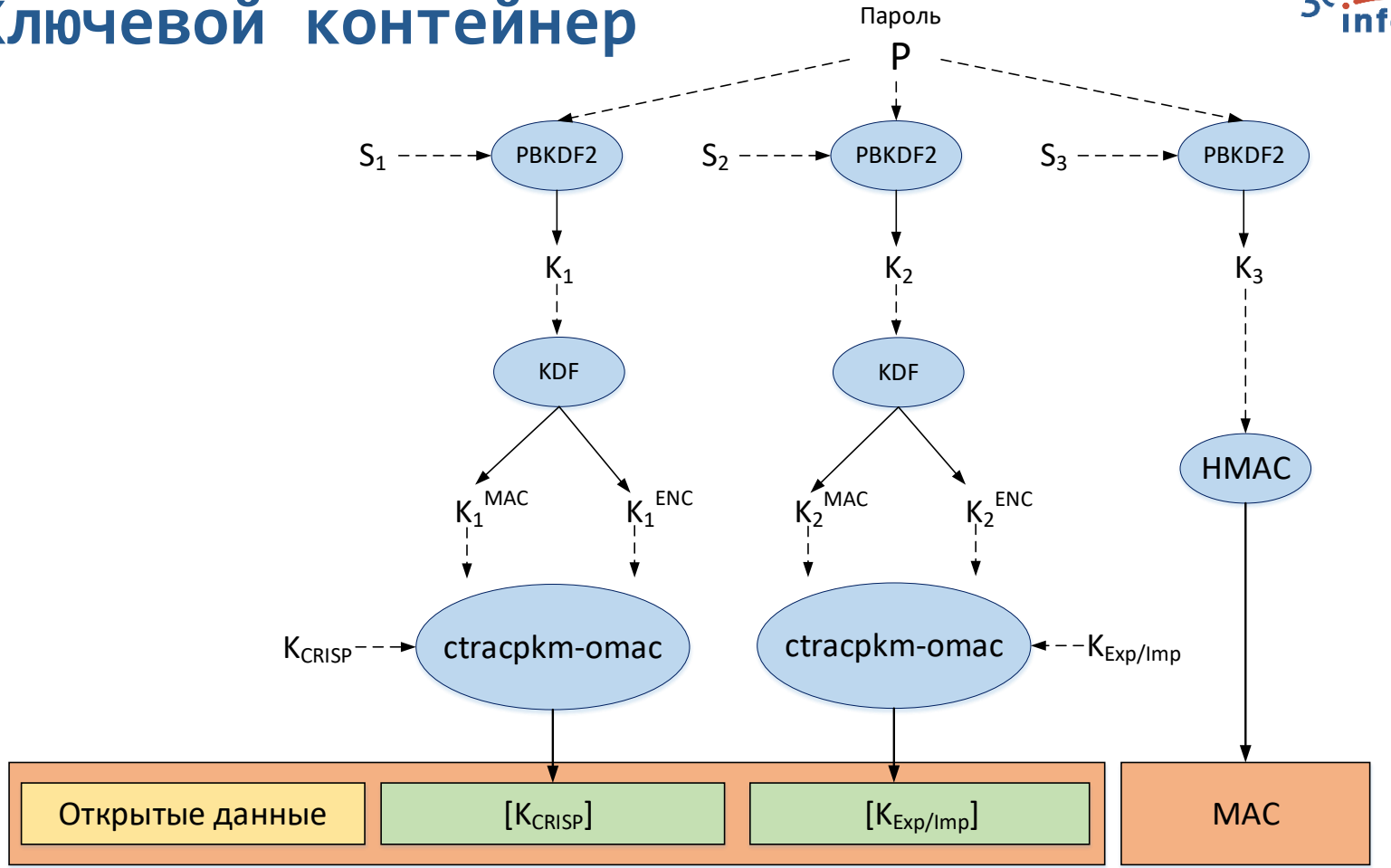
Доработки протокола ProtoQa

- изменен формат полей заголовка
- добавлена метки времени в заголовок
- процедура согласования параметров между участниками стала опциональной
- добавлена возможность указать желаемое время на обработку запроса ключа

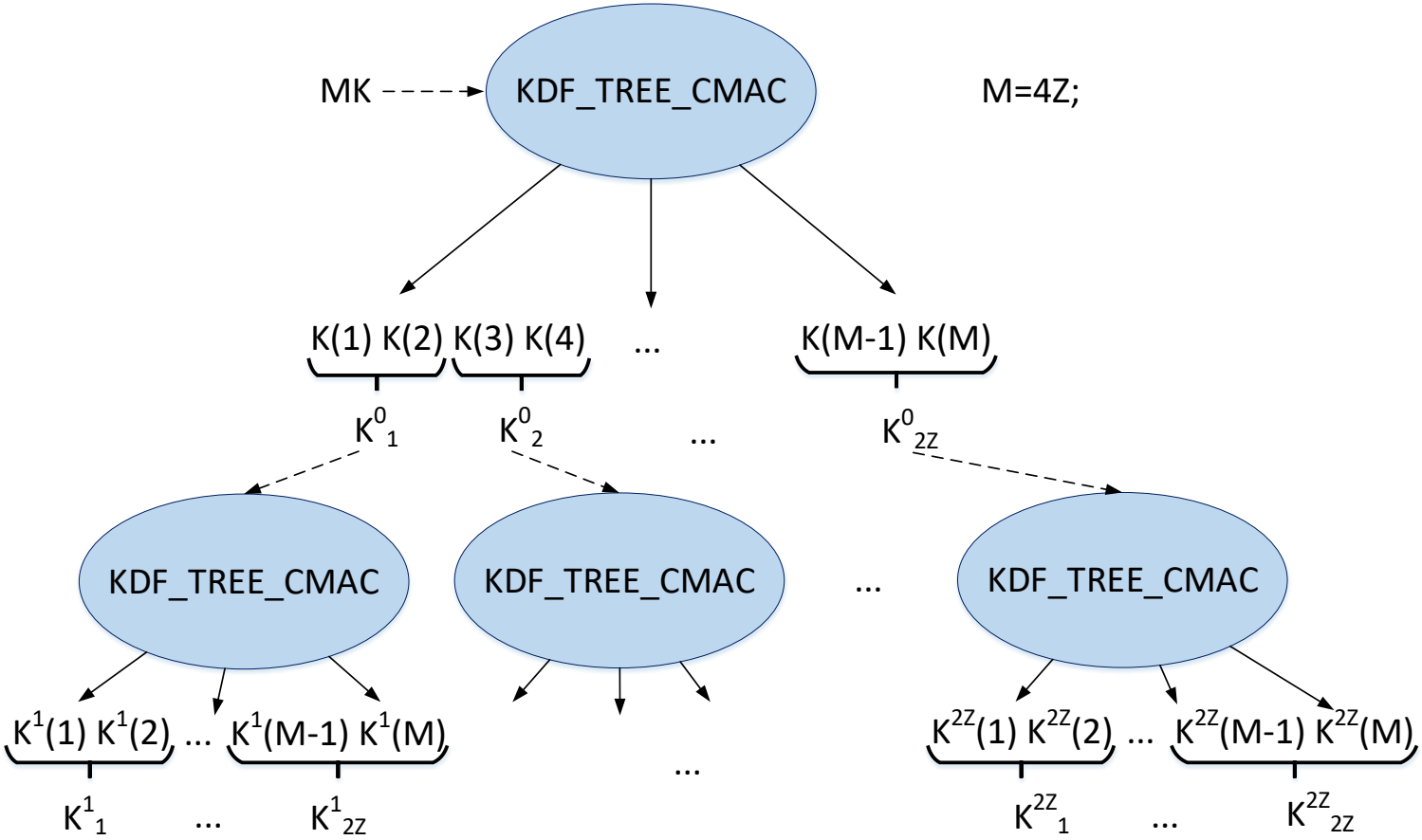
Доработки протокола ProtoQa

- уточнён раздел с условиями и ограничениями, накладываемыми на протокол
- добавлен справочный раздел, описывающий часть ключевой системы протокола

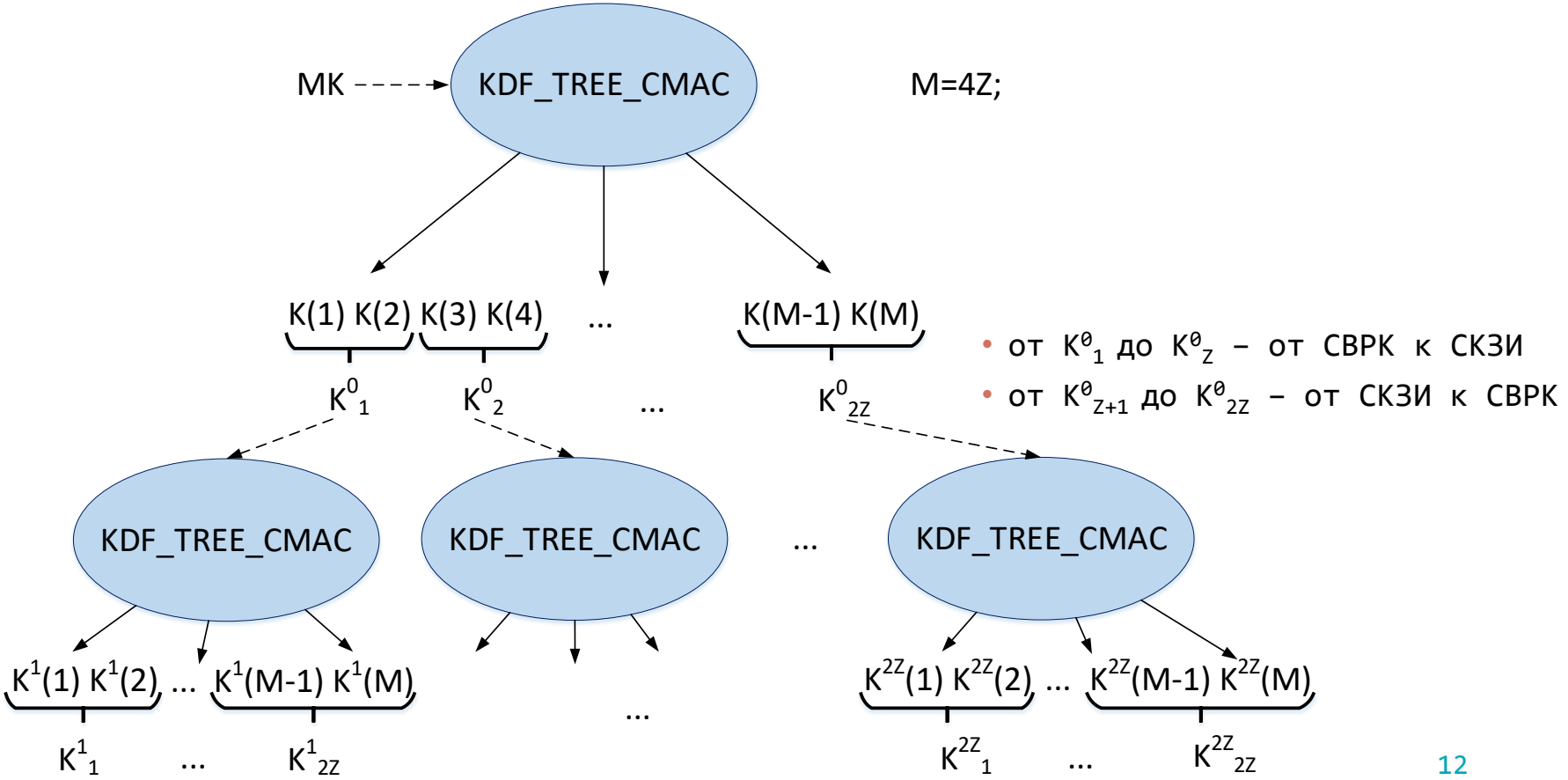
Ключевой контейнер



Производные ключи



Производные ключи

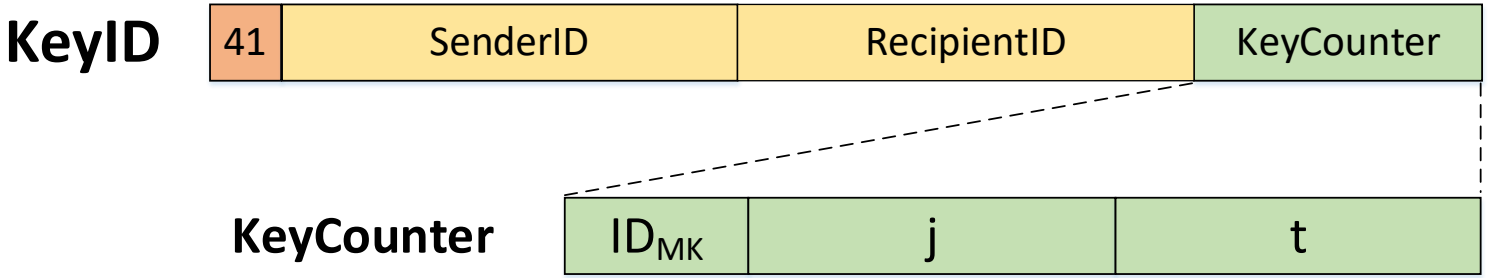


- от K^0_1 до K^0_Z – от СВРК к СКЗИ
- от K^0_{Z+1} до K^0_{2Z} – от СКЗИ к СВРК

Идентификаторы ключей

$$MK \rightarrow K^{j}_{t}$$

- **CRISP-сообщение:**



- **KExp/KImp:**

Обоснование стойкости. Ограничения

Число экспортируемых ключей K при одной и той же паре базовых ключей $(K_{MAC}^{Exp}, K_{ENC}^{Exp})$ не должно превышать:

– для шифра Магма $q \leq 2^{12}$;

– для шифра Кузнечик $q \leq 2^{45}$.

Число пар производных ключей (K_{MAC}, K_{ENC}), выработанных с использованием одного и того же базового ключа протокола CRISP в рамках реализации протокола ProtoOa, не должно превышать величины:

- для шифра Магма $q \leq 2^{15}$
- для шифра Кузнечик $q \leq 2^{46}$

Обоснование стойкости. Дополнительно

- рассмотрены различные модели действий нарушителя при атаке на функцию целостности передаваемых данных (имитозащиту)добавлена метки времени в заголовок
- сформулированы меры по защите от многократного навязывания
- показано, что использование механизма вложенных контейнеров на независимых ключах не ухудшает, а в ряде случаев и улучшает, защиту от злоумышленника

Ключевые система сетей защищенной связи на базе ККС ВРК с ДПУ

Принципы построения ключевой системы

- Общие ключи (КЗК) гибридные – ключи созданы с использованием двух независимых подсистем. Компрометация одной подсистемы не приведет к компрометации общего ключа
- Соединение физическим квантовым каналом возможно для некоторых пар узлов. Соединение логическим классическим каналом возможно для любой пары узлов
- Применение стандартизованных решений для уменьшения трудозатрат при сертификации и реализации сетей КРК

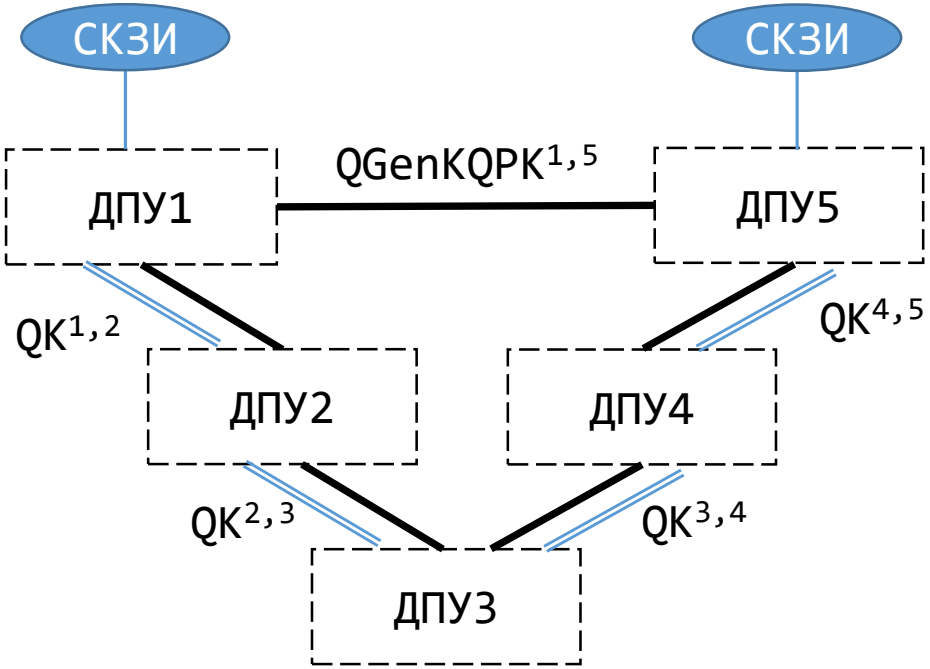
Принципы построения ключевой системы

- **ISTOQ-A** – Integral **ST**andard **O**f **Q**uantum keysystem – st**A**r
  - Централизованная сеть
  - Упрощенное создание общего ключа
  - Создание общего ключа для любой пары периферийных узлов
  - Возможность интеграции с сетью ISTOQ-M

- **ISTOQ-M** – Integral **ST**andard **O**f **Q**uantum keysystem – **M**ulti
  - Децентрализованная сеть
  - Масштабирование числа ДПУ в сети
  - Создание общего ключа для произвольной пары ДПУ

Ключевая система сети защищенной связи на базе ККС ВРК с ДПУ ISTOQ-M

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

Протокол выработки общего ключа Принципы

- КЗК создается из составляющих, каждая из составляющих суть ключевая информация
- Часть составляющих передается с защитой на классических ключах (выводятся из KGenKQPK классическими методами) – классические составляющие Rand
- Часть составляющих передается с защитой на квантовых ключах QK – квантовые составляющие Qrand
- Компрометация *отдельно* классических или квантовых ключей не приведет к компрометации КЗК

Протокол выработки общего ключа Криптографические алгоритмы

- Вывод ключей защиты составляющей КЗК Rand

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

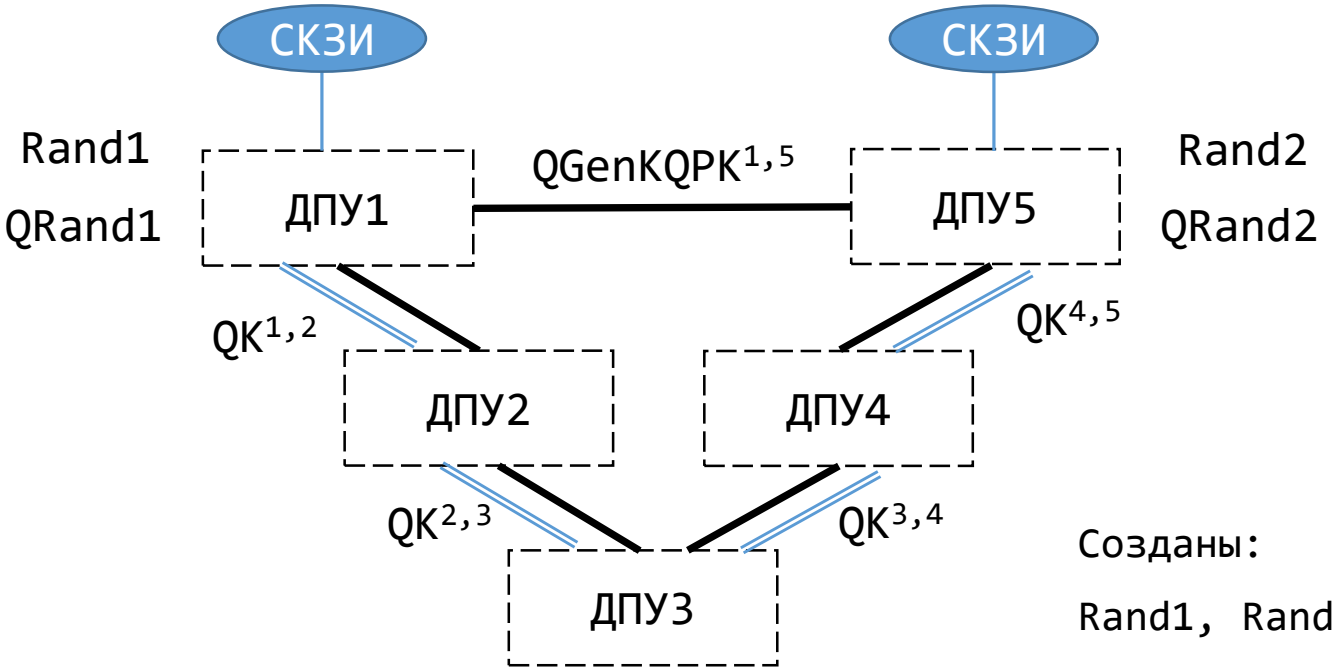
  - $seed = Counter_{K_i}$, $label = const$

- 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.

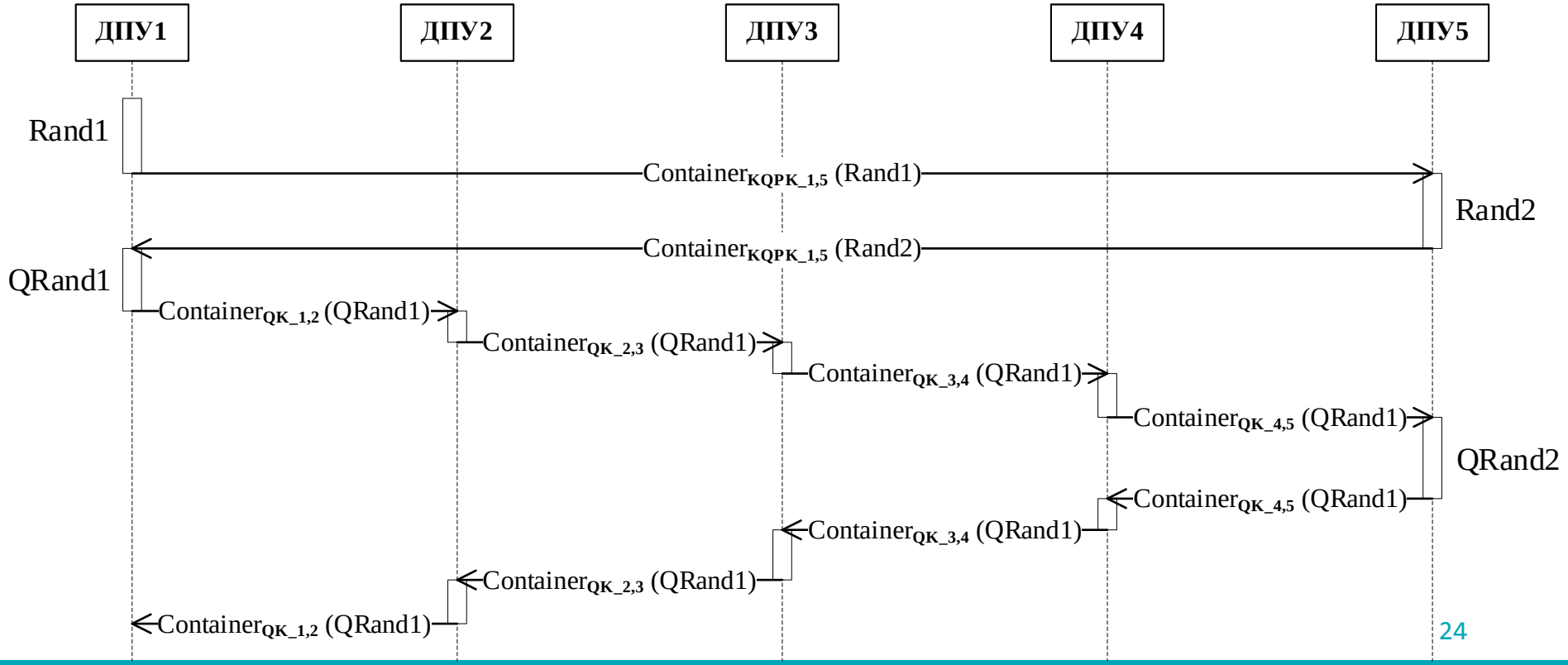
Протокол выработки общего ключа
Создание составляющих



Созданы:

Rand1, Rand2, QRand1, QRand2

Протокол выработки общего ключа
Передача составляющих



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 существует => существуют требуемые квантовые ключи
- Допустимо использование только составляющих Qrand => Составляющие КЗК Rand фиксированы (приложение А)

Протокол выработки общего ключа Обоснование. Обозначения

$n \in \{64, 128\}$ – битовый размер блока шифра;

$k = 256$ – битовый размер ключа;

t – вычислительная мощность противника (предельная трудоемкость осуществимой атаки);

q – число адаптивно выбираемых противником пар вход/выход (запросов к соответствующему «оракулу»);

σ – суммарное число n-битных блоков во всех сообщениях;

l_{max} – максимальное число блоков в одном сообщении;

l – битовая длина сообщения, $u = \lceil l/n \rceil$ – блоковая длина сообщения

Протокол выработки общего ключа Обоснование

Для шифров «Магма» и «Кузнечик» значение

$$\mathrm{Adv}^{PRP}_{\text{Магма}}(t,\sigma) \approx \frac{t}{2^k} \approx 0,\ \mathrm{Adv}^{PRP}_{\text{Кузнечик}}(t,\sigma) \approx \frac{t}{2^k} \approx 0$$

Преобладание противника для HMAC оценивается как

$$\mathrm{Adv}^{PRF}_{\text{HMAC-Стрибог-256}}(t,q,l_{\max}) \lessapprox \frac{t\cdot q}{2^{n-2}} + q\cdot l_{\max}\left(\frac{2t}{2^n} + \frac{2q^2}{2^{n+1}}\right) + \frac{3q^2}{2^{n/2+1}}$$

$$\approx \frac{t\cdot q\cdot l_{\max}}{2^{n-1}} + \frac{q^3\cdot l_{\max}}{2^n} + \frac{3q^2}{2^{n/2+1}},$$

Протокол выработки общего ключа Обоснование

Для функции KDF1 имеем

$$\mathrm{Adv}^{PRG}_{\mathrm{KDF1}}(t = 2^{128}) \lessapprox \frac{3 \cdot h \cdot t}{2^{k-2}} < \pi_{\mathrm{enc}}.$$

Для функции KDFG получаем

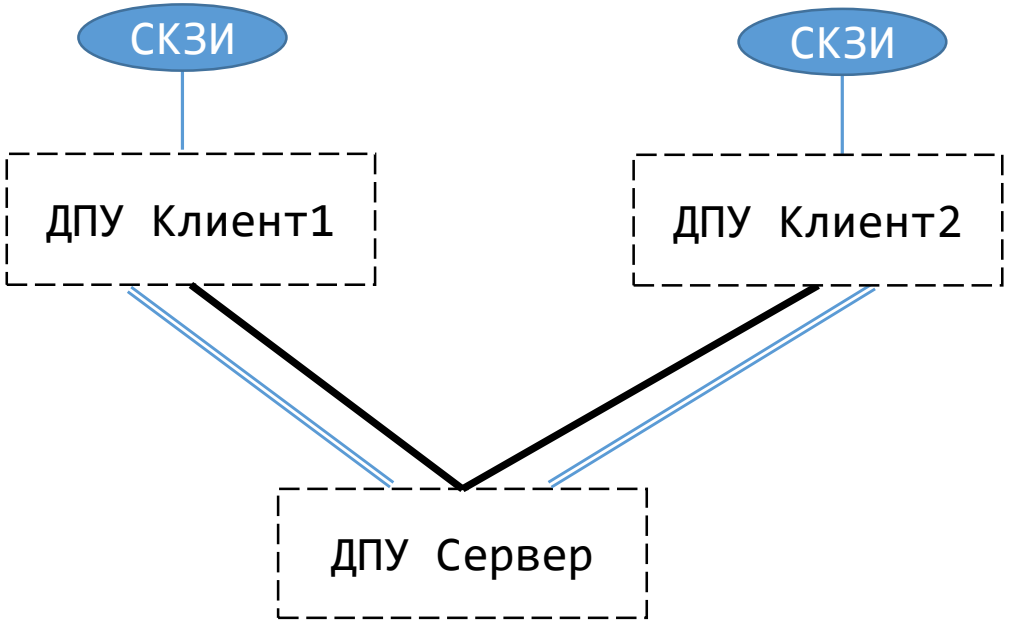
$$\mathrm{Adv}^{PRG}_{\mathrm{KDFG}}(t, M) \lessapprox \frac{13M^2 l}{2^{n-2}}.$$

Для функции KEXP15 имеем

$$\mathrm{Adv}^{DAE}_{\mathrm{K15}}(t, q) \approx \frac{4(qu)^2}{2^n} + \frac{(q(u+1))^2}{2^{n+1}} + \frac{q}{2^n} < \frac{5(qu)^2}{2^n}.$$

Ключевая система сети защищенной связи на базе ККС ВРК топологии «звезда» ISTOQ-A

Сеть топологии «звезда»



Центральный узел – ДПУ Сервер

Периферийные узлы – ДПУ Клиенты

ДПУ Клиенты связаны только с ДПУ сервером

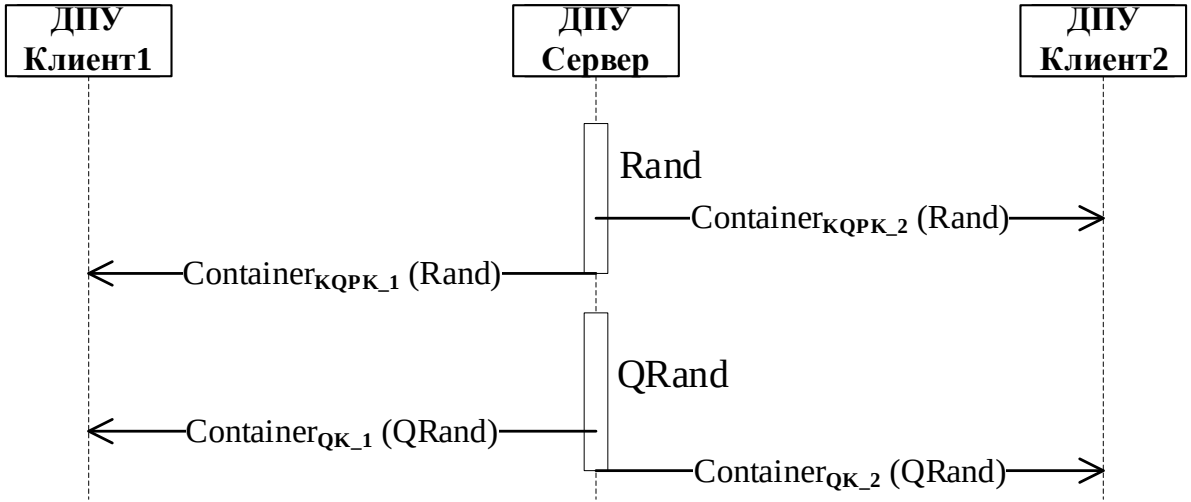
классический канал

квантовый канал

Протокол выработки общего ключа Криптографические алгоритмы

- Вывод ключей защиты составляющей КЗК Rand
  $\boldsymbol{KDF1}\left(KGenQPK_j^{t,Ser}\right) = KDF_{TREE\_256}\left(KGenQPK_j^{t,Ser}, label, seed, 1\right) = KQPK_j^{t,Ser} || KGenQPK_{j+1}^{t,Ser},$
  - $seed = Counter_{K_i}$, $label = const$
- Функция гибридизации
  $$\boldsymbol{KDFG}\left(Rand_n^{t,p}, QRand_n^{t,p}\right) = KDF(S, L, T, P, U, A) = QPK_n^{t,p} = \left\{QPK_n^{(1)\,t,p}, QPK_n^{(2)\,t,p}, \dots, QPK_n^{(M)\,t,p}\right\}$$
- Ключевые контейнеры:
  - CS_KW = 0 - KExp15-KImp15-Kuzn;
  - CS_KW = 1 - KExp15-KImp15-Magma.

Протокол выработки общего ключа
Передача составляющих



Созданы на Сервере:

Rand, QRand

Составляющие Rand, QRand на каждом ДПУ Клиенте

Смешиваются с помощью функции гибридизации KDFG

Протокол выработки общего ключа Особенности

- Маршрут создания КЗК однозначен для пары ДПУ Клиентов
- Связи ДПУ Клиентов друг с другом опциональны
- Явно выделяется центр управления сетью
- Централизованное создание КЗК – составляющие Rand, Qrand создает ДПУ Сервер =>
  - Уменьшение передачи ключевой информации по сети
  - Облегчение функции гибридизации KDFG
- Сохранены свойства базового протокола, кроме симметричности
- Заложена возможность интеграции подсети топологии «звезда» в сеть произвольной топологии

Протокол выработки общего ключа Обоснование. Рекомендации

1) Для обеспечения защиты от навязывания ложных сообщений при реализации ISTOQ-M/A в СВРК (СКЗИ) определенного класса с учетом эксплуатационных характеристик конечной системы, в которой предполагается использовать указанные изделия, рекомендуется ограничить максимальное количество сообщений с неправильной имитовставкой и/или выбирать приемлемую для данного класса СКЗИ длину имитовставки.

2) Число экспортируемых ключей K при одной и той же паре базовых ключей $(K_{MAC}^{Exp}, K_{ENC}^{Exp})$ не должно превышать:

– для шифра Магма $q \leq 2^{12}$;

– для шифра Кузнечик $q \leq 2^{45}$.

3) Число пар производных ключей (K_{MAC}, K_{ENC}), выработанных с использованием одного и того же базового ключа протокола выработки общего ключа парной связи между клиентами квантовой криптографической сети произвольной топологии/топологии «звезда», не должно превышать величины:

$$q \leq 2^{15}.$$

Протокол выработки общего ключа Обоснование. Выводы

При выполнении рекомендаций ключевые системы ISTOQ-M/A, определяющие процессы создания квантовозащищенных ключей квантовой криптографической сети (сети КРК) в произвольной топологии/топологии «звезда» обеспечивают конфиденциальность (при необходимости) и имитозащиту передаваемых данных, а также защиту от повторного навязывания передаваемых данных и навязывания ранее использованных ключей.

Окончательная оценка стойкости ISTOQ-M/A может быть получена только в рамках проведения тематических исследований конкретного СКЗИ и/или информационной системы, в которых реализована ключевая система.

Протокол выработки общего ключа Обоснование. Перспективы

Обоснование криптографических качеств ключевых систем Исток проведено также в терминах доказуемой стойкости, относительно противодействию *классическому* нарушителю (то есть была показана вычислительная стойкость).

В дальнейшем при подготовке заявки на рекомендации по стандартизации добавлена возможность применения криптографических примитивов, обладающих *абсолютной – теоретико-информационной* – стойкостью с сохранением базового фреймворка. В настоящий момент продолжается работа по обоснованию предлагаемых механизмов.

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow