УДК 004.056.5

А.Е. Жиляев

Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии

Квантовые ключи, создаваемые в результате выполнения протокола квантового распределения ключей, обладают абсолютной стойкостью в силу физических законов и не подвержены взлому даже при неограниченных вычислительных мощностях атакующего. Однако системы квантового распределения ключей имеют ограниченную дальность. Для преодоления проблемы максимальной дальности возможно построение сетей квантового распределения ключей на основе доверенных промежуточных узлов. В работе рассматривается связь магистральных сетей с сетями произвольной топологии, вводятся критерии классификации схем выработки и распределения ключей и проводится классификация некоторых схем по введенным критериям.

Ключевые слова: квантовое распределение ключей, сети КРК, классификация, квантовый ключ, квантовый маршрут.

DOI: 10.21293/1818-0442-2021-24-4-33-39

Развитие новых и совершенствование опробованных методов защиты информации связаны в первую очередь с ростом киберпреступлений в информационной сфере и расширением спектра угроз и рисков при атаках на информационные ресурсы. Это предопределят создание новых подходов к обеспечению информационной безопасности [1–5]. Перспективным подходом повышения уровня защищенности информации является применение и развитие систем квантового распределения ключей (КРК), которые позволяют создавать идентичные секретные ключи у двух географически разнесенных абонентов. Причем скорость создания таких ключей пусть и уступает скорости известных асимметричных алгоритмов, например схемы Диффи–Хелмана, но остается достаточно высокой для частой смены секретных ключей в средствах криптографической защиты информации (СКЗИ). Системы КРК могут использоваться в качестве замены доверенной доставки большого объема ключей курьером, т.е. исключается человеческий фактор из процесса распределения ключей [6].

Однако известны практические ограничения систем КРК, а именно предельная удаленность двух абонентов друг от друга, т.е. длина квантового канала, соединяющего абонентов [7]. Важно учитывать, что квантовый канал не может содержать активных оптических и электрооптических компонентов, в том числе усилителей сигнала, так как подобные элементы необратимо разрушают передаваемые квантовые состояния [8].

Известным и реализуемым с учетом настоящего уровня развития техники решением проблемы максимальной дальности в системах КРК является создание сетей КРК на основе доверенных промежуточных узлов (ДПУ). Концепция передачи квантового ключа по цепочке узлов, соединенных квантовыми каналами, была предложена в работах [9, 10]. Существенным недостатком такого подхода является требование доверия к промежуточным узлам, так как передаваемый ключ в открытом виде появляется на каждом ДПУ.

В настоящей работе покажем свойства возможных схем выработки и распределения ключей и предложим подход к классификации схем в зависимости от их параметров. Также покажем место известных схем выработки ключей согласно приведенной классификации и связь некоторых критериев классификации со свойствами безопасности, присущими этим схемам.

Связь сети произвольной топологии и магистральной сети

Задача создания общего ключа между двумя произвольными узлами сети КРК произвольной топологии в общем случае достаточно сложная [11]. Передача и/или создание ключа требует вычисления цепочки узлов, соединенных квантовыми каналами, через которые будет передаваться ключ или его составные части. Такую цепочку узлов будем называть квантовым маршрутом. Способ вычисления квантового маршрута не является предметом данной работы.

Для магистральной сети КРК, в которой два узла, формирующие общий ключ, соединены только одной цепочкой ДПУ, квантовый маршрут определяется однозначно. Для городских сетей распространенной является топология сети КРК «звезда» [12, 13], что позволяет оптимизировать число узлов в сети и уменьшить количество необходимых квантовых каналов. Такая сеть КРК состоит из выделенного узла в центре звезды и периферийных узлов. Каждый периферийный узел соединен квантовым каналом с центральным узлом. Общий ключ формируется для пар периферийных узлов. Для каждой пары периферийных узлов квантовый маршрут также определяется однозначно и состоит ровно из трех узлов: начинается на одном периферийном узле, проходит через центральный узел и заканчивается на втором периферийном узле из пары. То есть в сети топологии «звезда» можно однозначно выделить магистральную подсеть для любой пары периферийных улов.

В сетях произвольной топологии вычисление квантового маршрута также сводится к выделению некоторой магистральной подсети, соединяющей

два узла, формирующих общий ключ. Таким образом, задача создания общего ключа в произвольной сети КРК для некоторой фиксированной пары узлов сводится к задаче создания общего ключа в магистральной сети КРК. Далее будем рассматривать только способы создания общего ключа в магистральной сети КРК и их свойства.

Критерии классификации схем

Для формирования классификации схем выработки ключей предлагается рассматривать критерии двух категорий: критерии, связанные с конструкциями схем, и критерии, связанные с характеристиками полученной схемы.

Во-первых, схемы по своей конструкции существенно различаются по источнику ключа. Так, в сетях КРК, описываемых в документах ETSI [14] и ITU-T [15], предлагается использовать квантовый ключ, созданный на некотором сегменте сети. Однако каждый узел сети КРК, содержащий элементы аппаратуры КРК, обязательно содержит физический датчик случайных чисел, способный формировать ключевой материал для создания квантового ключа [16]. Этот датчик случайных чисел может использоваться и для создания общего ключа пары удаленных узлов. Соответственно, источником ключа может являться любой из узлов квантового маршрута. Выделим схемы, в которых источником ключа является оконечный узел, который формирует общий ключ, и схемы, в которых источник ключа расположен не на оконечных узлах квантового маршрута.

Следующим критерием для классификации схем является способ передачи созданной ключевой информации. Ожидаемый способ – последовательная передача по узлам, входящим в квантовый маршрут. Однако возможны схемы, создающие служебные, вспомогательные ключи защиты между узлами, не соединенными квантовым каналом, и использующие такие ключи для передачи ключевой информации, составляющей создаваемый общий ключ. То есть передача ключа может осуществляться по квантовому маршруту; по маршруту, полученному путем усечения квантового маршрута за счет создания вспомогательных ключей. Граничный случай – передача ключа напрямую между двумя оконечными узлами. Для единообразия дальнейшего описания будем считать прямой маршрут тривиальным вариантом усечения квантового маршрута.

Следующий критерий классификации относится к типу используемых методов защиты при передаче ключа по маршруту. Системы КРК создают квантовые ключи, стойкие в теоретико-информационном смысле [17, 18]. Потенциальный нарушитель при корректной реализации протокола КРК не способен узнать создаваемый квантовый ключ даже при наличии неограниченных вычислительных мощностей. Желательно, чтобы подобным свойством обладала схема создания ключа и для магистральной сети КРК, т.е. при передаче и формировании общего ключа использовались примитивы, обеспечивающие стойкость в теоретико-информационном смысле. Тогда результирующий общий ключ будет близок по своим свойствам к квантовому ключу, создаваемому на одном сегменте. Существенные объемы ключевого материала, которые потребуются для теоретико-информационно стойких примитивов, дают почву для создания схем, стойких в вычислительном смысле. То есть общий ключ формируется с применением вычислительно стойких примитивов [19].

Важным критерием является способ обработки ключевой информации на промежуточных узлах маршрута, который будет определять требования доверия к этим узлам. В идеальной модели доступ к ДПУ имеют только легитимные пользователи, и потенциальный нарушитель не может никаким образом узнать передаваемую ключевую информацию. Тогда специальная обработка передаваемой ключевой информации не требуется. Также возможны схемы, использующие дополнительные методы защиты, что предотвращает раскрытие ключевой информации на ДПУ при ее передаче по квантовому маршруту в различных моделях нарушителя: имеющего доступ в контролируемую зону, имеющего прямой доступ к памяти узла или узлов и др.

Отдельным блоком целесообразно рассматривать эксплуатационные критерии классификации, такие как скорость создания общего ключа (в некоторых элементарных операциях), величины дополнительных данных (оверхеда), передаваемых помимо самой ключевой информации.

Анализ некоторых известных схем

Далее приводятся некоторые известные схемы выработки и распределения общего ключа с последующей их классификацией согласно предложенным критериям.

Схема 1

Наиболее часто встречающаяся схема выработки общего ключа представлена на рис. 1.

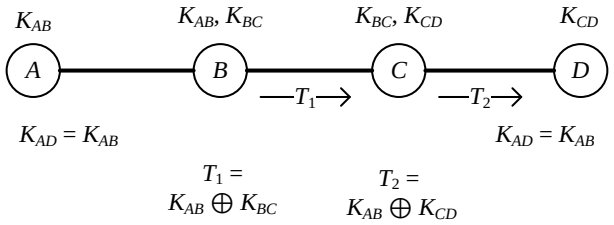

Рис. 1. Базовая схема выработки и распределения общего ключа

Ключ первого сегмента K_{AB} полагается общим ключом, который надо передать до второго оконечного узла. Защита при передаче от второго до последнего узлов осуществляется путем последовательного кодирования и декодирования одноразовым шифроблокнотом на квантовых ключах следующих сегментов K_{BC}, K_{CD} соответственно. В канале передаются закодированные сообщения T_1, T_2.

Схема 2

Модификация данной схемы, в которой в качестве общего ключа назначается квантовый ключ некоторого сегмента на квантовом маршруте, представлена на рис. 2. Оптимально с точки зрения скорости доставки общего ключа на оконечные узлы

выбирать квантовый ключ с сегмента, находящегося в середине квантового маршрута.

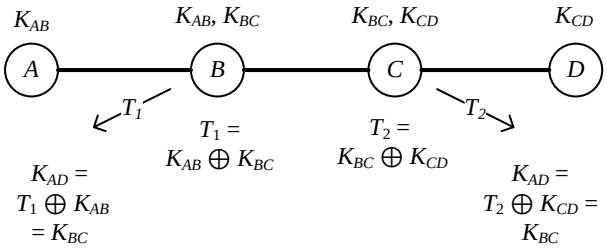

Рис. 2. Модифицированная схема выработки и распределения общего ключа

Схема 3

Представленные выше схемы не решают проблему раскрытия передаваемого ключа на промежуточных узлах. Рассмотрим некоторые подходы, позволяющие решить данную проблему. Следующая схема основана на соображениях, что одноразовый шифроблокнот (операция, исключающая ИЛИ) является линейным. Легко получить ключ совместного преобразования, а именно для некоторого ДПУ *i*-квантового маршрута ключ совместного преобразования получается по (1):

$$K_{(i-1,\, i+1)} = K_{(i-1,i)} \oplus K_{(i,i+1)}, \qquad (1)$$

где $K_{(i,j)}$ – ключ между узлами *i* и *j*.

За одно преобразование производится декодирование сообщения предыдущего сегмента с одновременным кодированием на ключе следующего сегмента. Общим ключом полагается некоторая случайная последовательность *X*, полученная с датчика случайных чисел ДПУ *A*. Схема изображена на рис. 3.

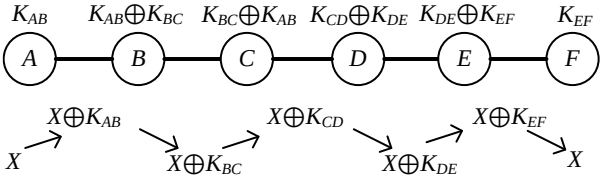

Рис. 3. Схема выработки ключа с созданием ключей совместного преобразования

ДПУ должны хранить только ключи совместного преобразования, безвозвратно удалив исходные квантовые ключи, из которых были получены эти ключи совместного преобразования. Эксплуатационные характеристики такой схемы оказываются существенно хуже, так как для каждого маршрута необходимо заранее подготовить и рассчитать ключи совместного преобразования. Если некоторый узел в сети соединен с *n* соседними узлами, то необходимо хранить C_n^2 ключей совместного преобразования вместо *n* квантовых ключей.

Схема 4

Реализация последовательного кодирования передаваемой ключевой информации совместно с использованными ключами порождает схему, описанную в патенте [20]. Схема представлена на рис. 4.

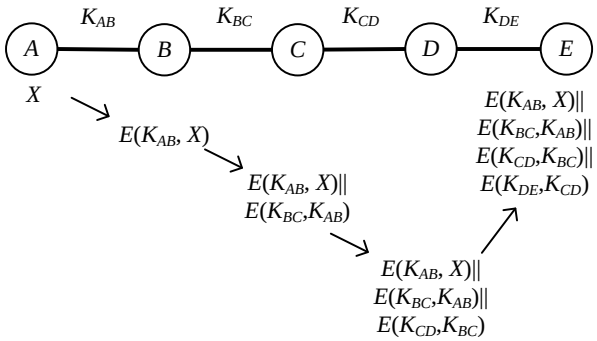

Рис. 4. Схема распределения общего ключа по принципу «матрешки»

Защита при передаче случайного числа, выступающего в качестве создаваемого общего ключа, осуществляется по принципу «матрешки». На первом узле случайное число кодируется функцией *E*() на первом квантовом ключе и полученное сообщение передается на второй узел. На втором узле ключ, использованный для кодирования на первом узле, кодируется функцией *E*() на квантовом ключе следующего сегмента и т.д. На последний узел квантового маршрута, состоящего из *r* узлов, поступает сообщение из *r*–2 сообщений, представляющих собой квантовый ключ некоторого сегмента, закодированный на квантовом ключе следующего сегмента, и одного сообщения, соответствующего закодированному случайному числу, из которого формируется общий ключ. Последний узел квантового маршрута последовательно декодирует части полученного сообщения, получая все необходимые ключи для декодирования случайного числа.

Несмотря на отсутствие требований к функции кодирования в описании [20], необходимо применять независимый набор квантовых ключей для каждого квантового маршрута даже при пересечении нескольких маршрутов на некоторых сегментах. При применении примитивов с теоретико-информационной стойкостью не возникает проблем повышенного расходования ключей, но с увеличением длины квантового маршрута необходимо передавать сообщения все большей длины.

Если достаточно обеспечивать вычислительную стойкость при передаче ключевой информации для формирования общего ключа, то для фиксированного квантового маршрута возможно однократно передать квантовые ключи всех сегментов на оконечный узел маршрута и в дальнейшем пересылать случайное число, закодированное квантовым ключом первого сегмента, напрямую на оконечный узел, минуя узлы квантового маршрута. С точки зрения стойкости схемы в целом это означает, что потенциальному нарушителю необходимо либо атаковать ключ кодирования первого сегмента (как единственное сообщение, появляющееся в открытом канале), либо реализовывать атаку на ДПУ для компрометации ключей защиты во время их передачи по квантовому маршруту. Причем в предложенной схеме на каждом следующем ДПУ маршрута раскрываются ключи со всех предыдущих сегментов маршрута.

Схема 5

Добавление ограничений на способ обработки ключевой информации на промежуточных узлах или на их структуру позволяет защититься от чтения передаваемой информации на промежуточных узлах потенциальным нарушителем. Так, способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей [21] накладывает специальное требование на используемые алгоритмы кодирования при передаче случайного числа. Используемые алгоритмы должны быть коммутативными. Для них должно выполняться свойство (2):

$$X = D_{K1}\left(E_{K1}\left(X\right)\right) = D_{K2}\left(E_{K2}\left(X\right)\right) = \\ = D_{K1}\left(D_{K2}\left(E_{K1}\left(E_{K2}\left(X\right)\right)\right)\right), \qquad (2)$$

где $D_{Ki}()$ – функция декодирования на ключе Ki; $E_{Ki}()$ – функция кодирования на ключе Ki; Ki – используемый ключ кодирования; X – передаваемое сообщение.

Тогда специальное устройство ДПУ и сохранение порядка преобразований позволяет добиться сокрытия передаваемых ключей на промежуточных узлах квантового маршрута. При этом не происходит увеличение расхода ключей защиты, отсутствует необходимость хранить большое количество различных ключей для различных вариантов маршрутов, а объем передаваемой закодированной информации по сегментам маршрута не увеличивается.

Для реализации способа требуется, чтобы каждый узел квантового маршрута помимо блоков квантовой аппаратуры (КА) имел независимые блоки СКЗИ, обозначены левый (Л) и правый (П) на рис. 5. Тогда последовательное кодирование полученного от предыдущего узла закодированного ключа C_i ключом следующего сегмента K_j в блоке П, передача промежуточного сообщения $C'_{i,j}$ в блок Л, декодирование на ключе предыдущего сегмента K_i в блоке Л и последующая передача закодированного передаваемого ключа C_j в блок П следующего узла квантового маршрута позволяет добиться защиты передаваемых данных на промежуточных узлах даже в случае, если потенциальный нарушитель обладает доступом к памяти одного из блоков узла.

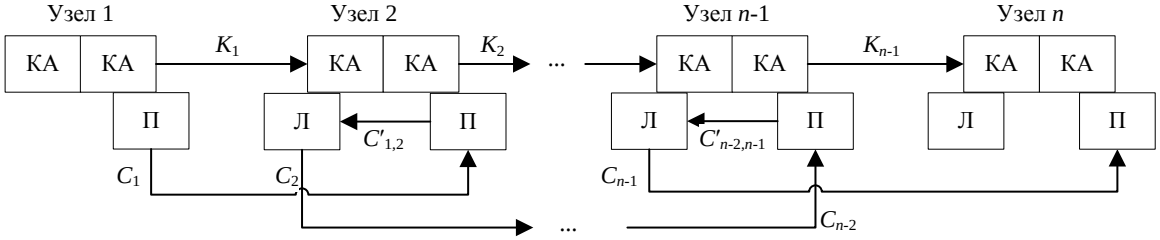

Рис. 5. Схема распределения общего ключа с фиксированным порядком преобразований

Схема 6

При наличии предварительно распределенного общего ключа между двумя оконечными узлами возможна реализация схемы со сквозной и транзитной защитой. Случайное число кодируется на предварительно распределенном ключе, получая таким образом некоторое защищенное представление случайного числа. Далее защищенное представление передается последовательно по узлам квантового маршрута с последовательной защитой на квантовых ключах каждого сегмента. В результате на промежуточных узлах маршрута возникает не само случайное число, формирующее общий ключ двух оконечных узлов, а только его защищенное представление. Даже имея прямой доступ к памяти промежуточного узла, становится невозможно получить непосредственно передаваемое случайное число.

Однако такая сквозная защита может быть реализуема и оправдана только для вычислительно стойких примитивов. Теоретико-информационно стойкие примитивы требуют однократного использования ключа защиты, следовательно, на оконечные узлы необходимо разместить достаточно большой запас предварительно распределенных ключей. В этом случае целесообразней не передавать никакой ключевой информации по сети, а использовать предварительно распределенные ключи в качестве общих ключей оконечных узлов. В то же время использование вычислительно стойких примитивов позволяет из малого объема предварительно распределенных ключей создавать значительно больший объем требуемых общих ключей.

В таблице приведена классификация описанных схем согласно предложенным критериям. Заметим, что для длинных квантовых маршрутов источник ключевой информации, расположенный на маршруте, практически не отличается от источника ключа, реализуемого протоколом КРК.

В настоящей работе рассматриваются только критерии, относящиеся к конструкции схем, так как для анализа эксплуатационных схем требуется дальнейшая конкретизация используемых алгоритмов. Указываются только некоторые важные эксплуатационные особенности.

Из таблицы видно, что схемы, предъявляющие меньше требований к используемым примитивам, не предоставляют защиты передаваемой ключевой информации на ДПУ и требуют повышенного доверия к ДПУ, что на практике приводит к реализации дополнительных организационно-технических мер защиты и особых правил размещения и/или эксплуатации ДПУ. Если схема обеспечивает защиту передаваемой ключевой информации, в том числе и при обработке на ДПУ, то появляются дополнительные ограничения к допустимым примитивам и ухудшаются эксплуатационные характеристики схемы.

Классификация схем по критериям, связанным с конструктивными особенностями

Критерий	Схема 1	Схема 2	Схема 3	Схема 4	Схема 5	Схема 6
Источник ключевой информации	Первый узел (квантовый ключ)	Произвольный узел (квантовый ключ)	Произвольный узел (случайное число)	Первый узел	Первый узел	Первый узел
Способ передачи	Последовательный от первого к последнему	Параллельный от источника до обоих оконечных	Последовательный от первого к последнему	Последовательная передача закодированных ключей совместно с закодированными ключами защиты по маршруту	Последовательно по маршруту. Специальный порядок обработки на ДПУ	Последовательно по маршруту
Класс используемых примитивов	Одноразовый шифроблокнот. Возможно применение произвольных алгоритмов	Одноразовый шифроблокнот. Возможно применение произвольных алгоритмов	Одноразовый шифроблокнот	Произвольные	Коммутативные	Вычислительно стойкие
Требование доверия к ДПУ	Максимальное	Максимальное	Среднее	Среднее	Минимальное	Минимальное
Эксплуатационные особенности	–	–	Предварительное вычисление всех ключей перекодирования. Повышенный объем хранимых ключей	Существенное повышение объема передаваемых данных при увеличении длины маршрута	Требуется контроль порядка обработки на ДПУ	Обязательны предварительно распределенные ключи на оконечных узлах

О влиянии источника ключевой информации

Отдельно отметим возможность навязывать общий ключ оконечных узлов узлом, на котором формируется исходная ключевая информация для дальнейшей передачи. Если такой узел-источник не совпадает ни с одним оконечным узлом, то допустимость такого навязывания определяется ожиданиями от конкретной сети КРК. Процессы, происходящие в сетях с централизованным управлением, более предсказуемы, но такой центральный узел требует максимальных усилий по его защите, и ему должны доверять все участники информационного взаимодействия. При этом любая схема, требующая передачи ключа строго от начала квантового маршрута в последний узел маршрута, адаптируется для централизованной сети КРК путем построения двух квантовых маршрутов и передачи одинаковых ключей до оконечных узлов от центрального узла.

В случае децентрализованных систем, где затруднительно выделить специальный узел и обеспечить для него высокую степень защиты, целесообразнее формировать ключевую информацию для создания общего ключа непосредственно на оконечном узле. Однако в этом случае оконечный узел может навязывать конкретные значения общего ключа, что может создать вектор атаки для потенциального нарушителя, если он сможет некоторым образом влиять на данный оконечный узел.

Решением проблемы является построение симметричных схем, в которых каждый из двух оконечных узлов вносит равный вклад в создание общего ключа. Фактически необходимо расширить схему создания ключа таким образом, чтобы каждый оконечный узел формировал свою часть ключевой информации, передавал ее второму оконечному узлу, после чего они независимо друг от друга объединяли две части ключевой информации для получения требуемого общего ключа. Правильный выбор способа объединения позволит исключить возможность навязывания и/или предсказывания итогового общего ключа любым из оконечных узлов до непосредственного формирования этого ключа.

Выводы

В работе предложены критерии для классификации схем выработки и распределения общих ключей для оконечных узлов магистральной сети КРК. Показана взаимосвязь процессов создания общих ключей в сетях КРК произвольной топологии с аналогичными процессами в магистральных сетях КРК. Проведена классификация некоторых схем выработки и распределения ключей в соответствии с предложенными критериями. Результаты анализа проведенной классификации показывают, что схемы с дополнительными ограничениями снижают требуемый уровень доверия к промежуточным узлам, но повышают эксплуатационные затраты или требуют специфичных реализаций системы КРК. Показаны возможные направления модификаций схем выработки и распределения ключей для улучшения их эксплуатационных свойств и свойств безопасности.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2020–2022 гг. (проект № FEWM-2020-0037).

Литература

1. Миронова В.Г. Реализация модели TAKE-GRANT как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов // Доклады ТУСУР. – 2011. – № 2(24), ч. 3. – С. 206–210.

2. Text marking approach for data leakage prevention / A.V. Kozachok, S.A. Kopylov, A.A. Shelupanov, O.O. Evsutin // Journal of computer virology and hacking techniques. – 2019. – Vol. 15, No. 3. – P. 219–232.

3. Shelupanov A. Threat model for IoT systems on the example of openUNB protocol / A. Shelupanov, A. Konev, T. Kosachenko, D. Dudkin // International Journal of Emerging Trends in Engineering Research. – 2019. – Vol. 7, No. 9. – P. 283–290.

4. Novokhrestov A.K. Model of threats to computer network software / A.K. Novokhrestov, A.A. Konev, A.A. Shelupanov // Symmetry. – 2019. – Vol. 11, No. 12. – P. 1506.

5. Актуальные направления развития методов и средств защиты информации / А.А. Шелупанов, О.О. Евсютин, А.А. Конев, Е.Ю. Костюченко, Д.В. Кручинин, Д.С. Никифоров // Доклады ТУСУР. – 2017. – Т. 20. – С. 11–24.

6. White Paper No. 27 Implementation Security of Quantum Cryptography. Introduction, challenges, solutions [Электронный ресурс]. – Режим доступа: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, свободный (дата обращения: 11.12.2021).

7. Испытание комплекса квантовой криптографической аппаратуры защиты информации на городских волоконно-оптических линиях связи / А.В. Борисова, А.Е. Жиляев, С.В. Алферов, В.Л. Елисеев, Ю.В. Кармазиков, А.Н. Климов, К.А. Балыгин // Вестник Российского нового университета. – Сер.: Сложные системы: модели, анализ и управление. – 2019. – № 4. – С. 100–110.

8. Молотков С.Н. О стойкости волоконной квантовой криптографии при произвольных потерях в канале связи: запрет измерений с определенным исходом // Письма в ЖЭТФ. – 2014. – Т. 100, вып. 6. – С. 457–464.

9. Elliot C. Building the quantum network // New Journal of Physics. – 2002. – Vol. 4. – P. 46.1–46.12.

10. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters / M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields // Nature. – 2018. – № 557. – P. 400–403.

11. Quantum Key Distribution: A Networking Perspective / M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, M. Voznak // ACM Comput. Surv. – 2021. – Vol. 53, No. 5. – P. 1–41.

12. Field and long-term demonstration of a wide area quantum key distribution network / S. Wang, W. Chen, Z.Q. Yin, H.W. Li, D.Y. He, Y.H. Li, Z. Zhou, X.T. Song, F.Y. Li, D. Wang // Optics Express. – 2014. – Vol. 22, No. 18. – P. 21739–21756.

13. Quantum key distribution network for multiple applications / A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami // Quantum Science and Technology. – 2017. – Vol. 2, No. 3. – P. 034003.

14. ETSI GS QKD 004 v.2.1.1 Quantum Key Distribution (QKD); Application Interface [Электронный ресурс]. – Режим доступа: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf, свободный (дата обращения: 11.12.2021).

15. ITU-T Recommendation Y.3800: Overview on networks supporting quantum key distribution [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/T-REC-Y.3800-202004-I!Cor1/en, свободный (дата обращения: 11.12.2021).

16. Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов / К.А. Балыгин, В.И. Зайцев, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2017. – Т. 106, вып. 7. – С. 451–458.

17. Bennet C.H. Quantum Cryptography: Public Key Distribution and Coin Tossing / C.H. Bennet, G. Brassard. // Theoretical Computer Science – 2014. –Vol. 560, Pt. 1. – P. 175–179.

18. Renner R. Security of Quantum Key Distribution [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/quant-ph/0512258.pdf, свободный (дата обращения: 11.12.2021).

19. Borodin M. Key generation schemes for channel authentication in quantum key distribution protocol / M. Borodin, A. Zhilyaev, A. Urivskiy // IET Quantum Communication. – 2021. – Vol. 2, No. 3. – P. 90–97.

20. Пат. 2 697 696 РФ, МПК H 04 L 9/08. Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей / А.М. Поздняков (РФ). – № 2 019 101 393; заявл. 18.01.19; опубл. 16.08.19, Бюл. № 23. – 3 с.

21. Пат. 2 708 511 РФ, МПК H 04 L 9/08, G 06 F 21/72. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей / А.Е. Жиляев (РФ). – № 2 019 102 923; заявл. 04.02.2019; опубл. 09.12.19, Бюл. № 34. – 2 с.

Жиляев Андрей Евгеньевич
Исследователь Центра научных исследований
и перспективных разработок АО «ИнфоТеКС»
Отрадная ул., 2Б, стр. 1, г. Москва, Россия, 127273
ORCID: 0000-0001-6717-1785
Тел.: +7-903-960-05-27
Эл. почта: Andrey.zhilyaev@infotecs.ru

Zhilyaev A.E.

Key generation and distribution schemes classification for quantum key distribution networks of arbitrary topology

Quantum keys created during the quantum key distribution protocol have absolute secrecy due to physical laws and are not susceptible to breaking even with the unlimited computing power of the attacker. However, quantum key distribution systems have a range limit. Quantum key distribution networks based on trusted intermediate nodes are built to overcome the problem of the maximum range. This paper examines the connection of backbone networks with networks of arbitrary topology, introduces criteria for the classification of key generation and distribution schemes, and classifies some schemes according to the criteria introduced.

Keywords: quantum key distribution, QKD network, classification, quantum key, quantum path.
DOI: 10.21293/1818-0442-2021-24-4-33-39

References

1. Mironova V.G., Shelupanov A.A., Yugov N.T. [Implementation of the TAKE-GRANT model as a representation of systems for differentiating access rights in an organization]. *Proceedings of TUSUR University*, 2011, no. 2(24), part 3, pp. 206–210 (in Russ.).

2. Kozachok A.V., Kopylov S.A., Shelupanov A.A., Evsutin O.O. Text marking approach for data leakage prevention. *Journal of Computer Mirology and Hacking Techniques*, 2019, vol. 15, no. 3, pp. 219–232. DOI: 10.1007/s11416-019-00336-9.

3. Shelupanov A., Konev A., Kosachenko T., Dudkin D. Threat model for IoT systems on the example of openUNB protocol. International *Journal of Emerging Trends in Engineering Research*, 2019, vol. 7, no. 9, pp. 283–290. DOI: 10.30534/ijeter/2019/11792019.

4. Novokhrestov A.K.,Konev A.A., Shelupanov A.A. Model of threats to computer network software. *Symmetry*, 2019, vol. 11, no. 12, p. 1506. DOI: 10.3390/sym11121506.

5. Shelupanov A.A., Evsyutin O.O., Konev A.A., Kostyuchenko E.Yu., Kruchinin D.V., Nikiforov D.S. [Current trends in the development of methods and means of information protection]. *Proceedings of TUSUR University*, 2017, vol. 20, pp. 11–24 (in Russ.).

6. ETSI White Paper No. 27 Implementation Security of Quantum Cryptography. Introduction, challenges, solutions. *ETSI*, 2018. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, free (Accessed: December 11, 2021).

7. Borisova A.V., Zhilyaev A.E., Alferov S.V., Eliseev V.L., Karmazikov U.V., Klimov A.N., Balygin K.A. [Testing of Quantum Key Distribution System in Urban Fiber-Optic Communication Lines]. *Vestnik ROSNOU: Complex systems: models, analysis, management*, 2019, no 4, pp. 100–110. DOI: 10.25586/RNU.V9187.19.04.P.100. (in Russ.).

8. Molotkov S.N. [On the stability of fiber-optic quantum cryptography at arbitrary losses in a communication channel: Exclusion of unambiguous measurements] *Jetp Letters*, 2014, vol. 100, no. 6, pp. 457–464 (in Russ).

9. Elliot C. Building the quantum network. *New Journal of Physics*, 2002, vol. 4, pp. 46.1–46.12.

10. Lucamarini M., Yuan Z.L., Dynes J.F., Shields A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 2018. no. 557, pp. 400–403. DOI: 10.1038/s41586-018-0066-6.

11. Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., Voznak M. Quantum Key Distribution: A Networking Perspective. *ACM Computing Surveys*, 2021, vol. 53, no 5, pp. 1–41. DOI: 10.1145/3402192.

12. Wang S., Chen W., Yin Z.Q., Li H.W., He D.Y., Li Y.H. , Zhou Z., Song X.T., Li F.Y., Wang D. Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express*, 2014, vol. 22, no 18, pp. 21739-21756. doi: 10.1364/OE.22.021739.

13. Tajima A., Kondoh T., Ochi T., Fujiwara M., Yoshino K., Iizuka H., Sakamoto T., Tomita A., Shimamura E., Asami S. Quantum key distribution network for multiple applications. *Quantum Science and Technology*, 2017, vol. 2, no. 3, p. 034003.

14. ETSI GS QKD 004 v.2.1.1 Quantum Key Distribution (QKD); Application Interface. *ETSI*, 2020. Available at: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf, free (Accessed: December 11, 2021).

15. ITU-T Recommendation Y.3800: Overview on networks supporting quantum key distribution. Available at: https://www.itu.int/rec/T-REC-Y.3800-202004-I!Cor1/en, free (Accessed: December 11, 2021).

16. Balygin K.A., Zaitsev V.I., Klimov A.N., Kulik S.P., Molotkov S.N. [Implementation of a quantum random number generator based on the optimal clustering of photocounts]. *Jetp Letters*, 2017, vol. 106, no 7, pp. 451–458. DOI: 10.7868/S0370274X17190109 (in Russ).

17. Bennet C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science*, 2014, vol. 560, part 1, pp. 175–179. DOI: 10.1016/j.tcs.2014.05.025.

18. Renner R. Security of Quantum Key Distribution, 2006. Available at: https://arxiv.org/pdf/quant-ph/0512258.pdf, free (Accessed: December 11, 2021).

19. Borodin M., Zhilyaev A., Urivskiy A. Key generation schemes for channel authentication in quantum key distribution protocol. *IET Quantum Communication*, 2021, vol. 2, no. 3, pp. 90–97. DOI: 10.1049/qtc2.12020.

20. Pozdnyakov A.M. Sposob peredachi soobshcheniya cherez vychislitel'nuyu set' s primeneniem apparatury kvantovogo raspredeleniya klyuchei [The way to transmit a message through the computational network using the quantum key distribution devices]. Patent RF, no. 2697696, 2019.

21. Zhilyaev A.E. Sposob formirovaniya klyucha mezhdu uzlami vychislitel'noi seti s ispol'zovaniem sistemy kvantovogo raspredeleniya klyuchei [The way to compute a key between nodes of the computational network using quantum key distribution systems]. Patent RF, no. 2708511, 2019.

Andrey E. Zhilyaev
Researcher, Research and Development Center,
JSC «InfoTeCS»
2B, Otradnaya st., bld.1, Moscow, Russia, 127273
ORCID: 0000-0001-6717-1785
Phone: +7-903-960-05-27
Email: Andrey.zhilyaev@infotecs.ru