УДК 004.056.5

А.Г. Втюрина, В.Л. Елисеев, А.Е. Жиляев, А.С. Николаева, В.Н. Сергеев, А.В. Уривский

Реализация средства криптографической защиты информации, использующего квантовое распределение ключей

Рассматриваются основные принципы построения комплексов защиты информации, допускающих автоматическое распространение и использование квантовых ключей. Рассматриваются неотъемлемые составные части, необходимые для функционирования такого комплекса в целом и аппаратуры распределения квантовых ключей в частности. В том числе обоснован выбор схемы аутентификации служебного канала квантовой аппаратуры, обоснован выбор квантового генератора случайных чисел и получен алгоритм его работы. Указаны проблемы совмещения шифраторов и квантовой аппаратуры и выявлены требования к логическому интерфейсу их взаимодействия. Также представлены результаты анализа влияния служебного трафика квантовой аппаратуры на нагруженность защищенного канала между шифраторами.

Ключевые слова: криптография, квантовое распределение ключей, квантовый генератор случайных чисел, аутентификация.

doi: 10.21293/1818-0442-2018-21-2-15-21

В современном мире наблюдается значительный рост скорости и объемов информации, передаваемой по каналам связи. В связи с продолжающимся переходом на электронные формы взаимодействия в России возрастают требования к обеспечению защиты информации. При этом необходимость обеспечения конкурентоспособности российской экономики, присутствия российских товаров и услуг на мировых рынках требует интеграции в международную сеть Интернет. Адекватной защитой от возрастающих рисков несанкционированного доступа к критически важной информации является использование шифрования. Однако в связи с отмечавшимся ранее ростом скорости передачи данных появляется проблема быстрой выработки нагрузки на ключ и необходимости частой смены ключа шифрования.

Другим риском является создание эффективного квантового компьютера, что потенциально снижает стойкость асимметричных криптографических алгоритмов и алгоритмов выработки симметричного ключа, основанных на задачах факторизации и дискретного логарифмирования, в связи с возможностью применения квантового алгоритма Шора [1].

Одним из возможных решений поставленных проблем является применение квантового распределения ключей (КРК) как средства доставки симметричных ключей абонентам [2]. Однако необходимо обеспечить тесную взаимосвязь шифраторов и аппаратуры квантового распределения ключей для синхронной смены ключей шифрования и безопасной бесперебойной поставки данных ключей от квантовой аппаратуры. Более того, так как параметры оптоволокна, в котором реализуется квантовый канал связи (ККС), постоянно изменяются в зависимости от условий окружающей среды и это влияет на распространение лазерных импульсов в квантовом канале связи, то при квантовом распределении ключей в условиях рабочей эксплуатации необходима своевременная подстройка параметров аппаратной части аппаратуры КРК, что возможно только в автоматическом режиме.

Компания «ИнфоТеКС» совместно с лабораторией квантовых оптических технологий МГУ в рамках проекта Минобрнауки РФ (проект 03.G25.31.0254) разрабатывает комплекс квантовой криптографической аппаратуры защиты информации (ККА ЗИ) ViPNet Quandor (рис. 1), в котором учтено решение описанных выше проблем и который будет обеспечивать передачу информации по сетям связи общего пользования, используя квантовый принцип распределения симметричных ключей шифрования [3]. Данный ККА ЗИ структурно состоит из двух взаимосвязанных составных частей:

– автоматической аппаратуры квантового распределения ключей (АА КРК);

– квантово-криптографического шифратора (ККШ).

Пользовательские данные из доверенной среды передачи (ДСП) передаются в зашифрованном виде между сопряженными ККШ в сети связи общего пользования.

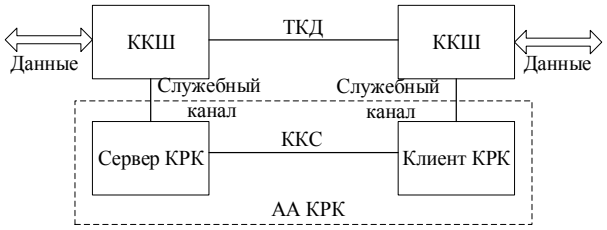

Рис. 1. Общая схема ККА ЗИ ViPNet Quandor

Для организации транспортного канала данных (ТКД) с использованием квантовых ключей необходимо наличие двух сопряженных составных частей АА КРК: сервера КРК и клиента КРК, а также двух ККШ. При этом на одной стороне располагается один ККШ и сервер КРК, а на другой стороне – другой ККШ и клиент КРК. Два ККШ соединяются ТКД, а сервер КРК и клиент КРК – квантовым каналом связи. Составные части АА КРК и ККШ на каждой из сторон ТКД связаны друг с другом служебным каналом, который позволяет ККШ получать

квантовые ключи (КК) и осуществлять операции по запросу АА КРК. Плановые характеристики разрабатываемого комплекса: скорость передачи данных в ТКД – 10 Гбит/с, при этом обеспечение конфиденциальности информации по ГОСТ Р 34.12–2015, а скорость выработки квантовых ключей не менее 256 бит в минуту.

Существенные составляющие АА КРК

Рассмотрим неотъемлемые компоненты АА КРК и общие принципы их взаимодействия.

Работа любой АА КРК определяется используемым протоколом квантового распределения ключей (протокол КРК). Обязательными этапами в любом протоколе КРК являются:

1. Предварительная настройка квантового канала связи.

2. Кодирование ключевой информации в одиночные фотоны и передача данных фотонов через квантовый канал связи. Неотъемлемой частью АА КРК является генератор случайных чисел, необходимый для выработки ключевой информации для кодирования фотонов.

3. Постобработка полученной ключевой информации (в том числе исправление ошибок в принятой и переданной последовательностях, усиление секретности очищенных последовательностей) с использованием классического канала. При этом неотъемлемой частью любой АА КРК является построение классического аутентифицированного канала для передачи служебного трафика по постобработке полученной ключевой информации.

Физическими законами обеспечивается неперехватываемость информации, передаваемой в квантовом канале связи. Можно выделить несколько типов кодирования ключевой информации в фотоны. Так, известный протокол BB84 использует поляризационное кодирование [4], что непременно повлечет использование специализированного оптоволокна, сохраняющего поляризацию. Иное оптическое волокно не сохраняет состояние поляризации, поэтому при прохождении через линию связи поляризация квазиоднофотонных состояний неконтролируемым способом изменяется. Хотя эти изменения достаточно медленные, все равно необходима активная стабилизация поляризации. Попытки реализовать такие системы были, но не получили дальнейшего развития из-за сложности стабилизации.

Поэтому в проекте выбрано фазовое кодирование, при котором биты исходной ключевой информации кодируются в относительную фазу двух когерентных разделенных во времени квазиоднофотонных состояний. В таких системах КРК при детектировании информационных квантовых состояний используется интерферометр Маха–Цандера, на котором «сбивается» пара пространственно разнесенных квазиоднофотонных когерентных состояний с различной относительной фазой [5]. Пространственное разнесение состояний производилось на таком же интерферометре Маха–Цандера.

Для получения стабильной интерференционной картины важно, чтобы относительная разность длин плеч интерферометров была одинаковой. Основные способы балансировки предполагают прерывание передачи ключей в режиме квазиоднофотонных состояний, перевод системы в классический режим и посылки одинаковых состояний для того, чтобы сбалансировать интерферометр [6]. Смена режима работы лазера и прерывание передачи негативно скажутся на времени выработки квантового ключа. Также данный метод балансировки требует дополнительной передачи служебных команд через классический аутентифицированный канал.

В целях ускорения выработки квантовых ключей целесообразно сократить число переключений режимов работы лазера. Для этих целей возможно применение альтернативного способа балансировки, не требующего дополнительного трафика в служебном канале, основанного на внесении дополнительной контролируемой фазы в одно из плеч интерферометра принимающей стороны, так как замечено, что отклонение видности интерференционной картины от идеальной однозначно связано с регистрируемой разностью числа нулей и единиц в просеянном ключе, т.е. в совпадающих базисах. Поэтому можно осуществлять балансировку только в квазиоднофотонном режиме, используя разность числа нулей и единиц в просеянном ключе как сигнал ошибки Q в качестве сигнала обратной связи. Это сокращает время балансировки и, кроме того, не требует дополнительного обмена по открытому каналу связи. Поскольку видность интерференционной картины определяется относительной разностью длин плеч интерферометров в сервере КРК и клиенте КРК, то достаточно регулировать только один из интерферометров.

Согласно результатам экспериментов [7] время разбалансировки интерферометров на величину, дающую чувствительный вклад в ошибку ключа, иногда оказывается сравнимо со временем его генерации. Это означает, что регулировка фазы должна производиться чаще, чем вырабатывается сигнал ошибки (просеянный ключ).

Таким образом, чтобы обеспечить равенство длин плеч интерферометров без постоянного их измерения, необходимо постоянно изменять фазу, интерполируя эту подстройку фазы между редкими моментами измерения разности длин плеч. То есть необходимо определить усредненную за некоторое время скорость изменения фазы и в промежутках между моментами регулирования изменять фазу с этой скоростью.

Особенности аутентификации при квантовом распределении ключей

Как обозначалось ранее, неотъемлемой частью АА КРК является построение классического аутентифицированного канала для передачи служебного трафика.

Обычно для аутентификации первой сессии выработки первичных квантовых ключей должны использоваться предварительно распределенные симметричные ключи. При накоплении достаточного количе-

ства квантовых ключей аутентификация продолжается на этих квантовых ключах, полученных от АА КРК.

Существует два основных подхода к аутентификации классического канала в системах КРК. Возможно применение либо теоретико-информационно стойкой, либо вычислительно стойкой аутентификации. Применение теоретико-информационно стойкой аутентификации, несмотря на более высокий уровень стойкости, связано с рядом существенных проблем.

Ключевой проблемой теоретико-информационно стойкой аутентификации является необходимость использования новых различных ключей аутентификации для каждого аутентифицируемого сообщения [8]. При этом ключ на аутентификацию последующей сессии выработки квантовых ключей принято отрезать от текущего общего квантового ключа, выработанного в результате протокола КРК. Таким образом, в зависимости от объемов трафика, который необходимо аутентифицировать, возможна ситуация, при которой большая часть выработанного квантового ключа будет отрезана на аутентификацию канала для последующей серии.

В качестве теоретико-информационной стойкой аутентификации принято применять функции универсального хэширования [9]. Характеристики наиболее перспективных классов функций универсального хэширования приведены в [10]. Нижняя оценка для длины ключа аутентификации таких функций – двоичный логарифм от длины сообщения. Так, для аутентификации хэш-функциями на базе кодов Рида–Соломона, обладающей одной из минимальных длин необходимого ключа аутентификации, для аутентификации 3,5 Мбит трафика, переданного в ходе работы протокола КРК, разработанного в рамках проекта, необходимо 236 бит ключа аутентификации при ожидаемой производительности данного протокола 256 бит ключа. Следовательно, почти весь вырабатываемый ключ будет отводиться на аутентификацию следующей сессии выработки, что малоцелесообразно.

Таким образом, для квантовых криптографических систем, обладающих небольшой скоростью генерации ключей из-за высокого уровня стойкости вырабатываемых КК, применение теоретико-информационной аутентификации оказывается невозможным. Для таких систем остается применение вычислительно стойкой аутентификации. При этом в отличие от первого подхода на одном ключе аутентификации допустимо аутентифицировать несколько сообщений.

Необходимость и базовые принципы квантового генератора случайных чисел

Неотъемлемой частью АА КРК является генератор случайных чисел (ГСЧ) для получения случайных последовательностей. Для обеспечения секретности вырабатываемых квантовых ключей необходимо использование случайных чисел, полученных исключительно с физических генераторов [11]. При этом необходимо использовать именно квантовые генераторы случайных чисел (КГСЧ). Результаты измерений над квантовой системой, приготовленной каждый раз в одном и том же состоянии, носят принципиально случайный характер. Поэтому истинная случайность имеет место только в квантовой области.

Наиболее целесообразным способом получения первичной случайности можно считать способ, основанный на принципе фотодетектирования [12]. Финальная случайная последовательность нулей и единиц возникает в результате измерений над квантовой системой и последующей обработки результатов этих измерений. Для грамотного исполнения КГСЧ необходимо утвердить следующие важные этапы работы КГСЧ:

1. Выбрать способ фотодетектирования, который бы контролируемым образом обеспечивал независимость отдельных актов регистрации и приводил к пуассоновской статистике фотоотсчетов.
2. Выбрать такую группировку фотоотсчетов в отдельные блоки, которая бы обеспечивала извлечение всей случайности, которая содержится в процессе регистрации квантовых состояний.
3. Выбрать такой способ постобработки, который бы гарантировал получение идеально случайной последовательности, а не близкой к идеальной.

Фотодетектирование по своей природе является квантовым процессом, поэтому оно используется многими авторами при разработке КГСЧ. При фотодетектировании возникает распределение Ферми–Дирака [13] при «размещении» фотоотсчетов по временным интервалам.

Получение истинно случайной последовательности из последовательности фотоотсчетов означает отображение последовательностей фотоотсчетов длиной в n тактов с m отсчетами в истинно случайные блоки нулей и единиц длиной l, зависящей от n и m: $\{*,\_\}^{n_m} \to \{0,1\}^l$, $(1<n)$. Последовательность разбивается на ходу на блоки длиной n, содержащие одинаковое число тактов. В каждом блоке может быть m фотоотсчетов (*), $0 \le m \le n$. Всего типов таких блоков существует $2n$. Вероятность последовательности с m отсчетами (*) и n–m-пропусками (_) имеет вид $(1-p(*))^{n-m}\,p(*)^m$. При этом полное число равновероятных последовательностей (последовательностей, содержащих одинаковое число тактов с отсчетами (*) и пустых тактов (_)) одного класса равно C_n^m.

Согласно [14] необходимо пронумеровать все равновероятные последовательности из одного класса, а затем извлечь блок случайных нулей и единиц из двоичного номера последовательности в данном классе. При прямом способе нумерации сама последовательность является адресом номера в данном классе. Однако в этом случае размер адресной таблицы будет экспоненциально велик. Например, при длине обрабатываемого блока в 64 такта размер адресной таблицы составит $2^{64} \approx 10^{19}$, что практически нереализуемо. Поэтому предлагается использо-

вать методы арифметического кодирования, а именно способ нумерации последовательностей фотоотсчетов, требующий лишь полиномиальных ресурсов по длине последовательности и позволяющий обрабатывать последовательности практически любой длины [15].

Пусть в последовательности имеется K отсчетов (*). Тогда есть взаимное однозначное соответствие между последовательностью фотоотсчетов (i_1, i_2, …, i_n) и ее номером:

$$\mathrm{Num}(i_1,i_2,...,i_n)(0\le \mathrm{Num}(i_1,i_2,...,i_n)\le C_n^K-1):$$

$$\mathrm{Num}(i_1,i_2,...,i_n)=C^1_{j_1-1}+C^2_{j_2-1}+...+C^k_{j_k-1},$$

$$C^1_{j_1-1}=0,\quad j<l. \qquad (1)$$

В формуле (1) индексом j_k обозначен номер позиции.

В результате разработки АА КРК был получен следующий алгоритм работы КГСЧ:

1. Биномиальные коэффициенты вычисляются заранее и помещаются в таблицу размером $n\times n$ в память вычислительного устройства, например, системы на модуле, содержащей FPGA (рис. 2).

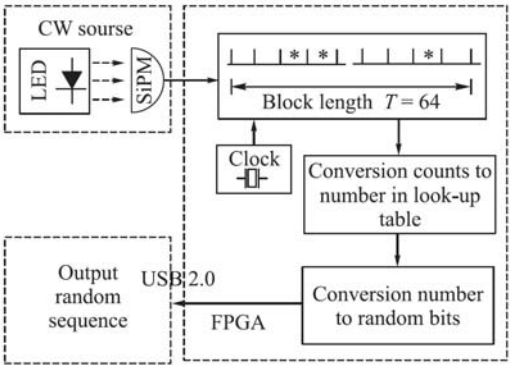

Рис. 2. Блок-схема функционирования КГСЧ

2. При появлении первого отсчета в позиции j_1 выбирается биномиальный коэффициент на пересечении первой строки j_1 и первого столбца матрицы. При появлении второго отсчета выбирается коэффициент в матрице на пересечении j_2 строки и второго столбца матрицы. В итоге получается номер последовательности $\mathrm{Num}(i_1,i_2,...,i_n)$.

3. Номера последовательностей находятся в пределах $0<\mathrm{Num}<N_k-1$, причем бинарное представление числа последовательности в классе $N_k=\sum_{i=0}^{i_{\max}}2^{k_i}$. Необходимо рекурсивно выдать блок случайных нулей и единиц. Если номер текущей последовательности Num находится в интервале $2^{k0}+2^{k1}+...+2^{k_{i-1}}\le \mathrm{Num}\le 2^{k0}+2^{k1}+...+2^{k_{i-1}}+2^{k_i}-1$, причем $i\le i_{\max}$, тогда выходной случайной последовательностью будет k_i младших разрядов бинарного представления Num. Число номеров последовательностей в этом диапазоне равно 2^{k_i}.

Замечательно, что использование подобного способа экстракции случайной последовательности дает истинно случайную последовательность. Единственным условием становится пуассоновский характер последовательности фотоотсчетов, что может быть достигнуто точностью практической реализации КГСЧ.

Как видно из схемы, представленной на рис. 2, КГСЧ состоит из трех элементов:

– генератора случайных импульсов (источник излучения LED, матрица SiPM);

– блока обработки на основе вычислительного устройства (FPGA), в котором реализованы алгоритмы КГСЧ-группировки фотоотсчетов, постобработки полученной последовательности и выдачи их потребителю;

– интерфейса для подключения внешнего потребителя получаемой последовательности случайных чисел (Output random sequence).

Интерфейс взаимодействия ККШ и АА КРК

Для практической реализации КККА ЗИ с использованием КРК немаловажным аспектом является грамотное согласование АА КРК и ККШ, в которые будут передаваться квантовые ключи.

Протокол их взаимодействия необходимо разрабатывать универсальным, чтобы не создавать жесткой привязки шифраторов к серверу КРК или клиенту КРК.

Самодостаточная квантовая аппаратура, которая самостоятельно строит для себя классический аутентифицированный канал, вызывает ряд проблем при практическом использовании, а именно необходимость маршрутизации отдельного канала служебного трафика и необходимость обеспечения защиты передачи квантовых ключей в шифраторы, что ведет к созданию и контролю сложных криптографических преобразований в квантовой аппаратуре. Поэтому целесообразно строить данный канал непосредственно внутри комплекса защиты информации, т.е. через шифратор.

Таким образом, можем выделить минимально необходимый состав трафика, проходящего между АА КРК и ККШ, а также обозначить требования, которые необходимо обеспечить при прохождении данного трафика.

1. В канале между АА КРК и ККШ передаются полученные готовые квантовые ключи. Криптографические ключи, в том числе и КК, должны передаваться только по защищенным каналам. В случае с передачей квантовых ключей защита должна осуществляться с помощью шифрования. Следовательно, стоит учитывать необходимость выделения ключей для шифрования квантовых ключей при передаче, что несомненно вызовет существенные изменения в общей ключевой системе комплекса. Более того, для бесперебойной работы шифраторов следует передавать ключи в приоритетном порядке.

2. Вторым важным типом трафика является служебный трафик АА КРК, которым обменивается аппаратура при постобработке переданной ключевой

последовательности. Протоколы КРК накладывают только требование аутентификации на данный трафик, поэтому шифровать служебный трафик не обязательно. Важно, чтобы ККШ по возможности без задержек передавал служебный трафик по каналу и дальше в АА КРК. С точки зрения интерфейса между АА КРК и ККШ данный трафик – данные, которые необходимо оперативно передать без изменений и какой-либо обработки.

3. Стоит учитывать, что создание комплекса защиты информации, а не применение отдельных шифратора и квантовой аппаратуры позволяет наладить тесное взаимодействие устройств, что в свою очередь выльется в появление сервисного трафика между ККШ и АА КРК. Таким образом, АА КРК и ККШ способны отслеживать работоспособность друг друга и, более того, оценивать возможность возобновления работоспособности в зависимости от типов ошибки.

Деградация канала ТКД

Стоит отметить, что в связи с появлением дополнительного для ККШ трафика, а именно служебного трафика АА КРК, важной частью разработки комплекса является согласованное использование транспортного канала полезной нагрузкой и служебным трафиком АА КРК. В рамках проекта была оценена деградация ТКД при различных ограничениях полосы пропускания служебного трафика.

Были проведены исследовательские испытания по выявлению величины падения скорости передачи данных в ТКД из-за добавления служебного трафика АА КРК. На рис. 3 представлен график зависимости падения скорости передачи данных в ТКД в виде деградации ДСП от длины квантового канала связи (ККС).

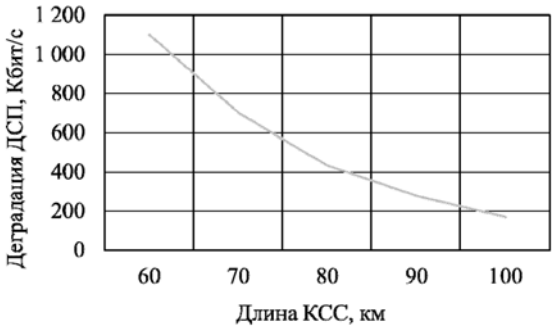

Рис. 3. График зависимости падения скорости передачи в ДСП

Из графика видно, что наибольшее падение скорости передачи данных в ДСП наблюдается при длине ККС 60 км, при которой объем данных, передаваемых по каналу служебной связи, максимальный для постобработки переданной ключевой информации. Тем не менее максимальная величина падения скорости передачи полезных данных в ДСП составляет – 1,1 Мбит/с при скорости ТКД 10 Гбит/с, что составляет 0,011% от скорости ТКД.

По результатам анализа исследовательских испытаний следует, что падение скорости передачи данных в ДСП составляет 0,011%. Таким образом, при использовании КРК для защиты высокоскоростных каналов передачи можно не ограничивать скорость служебного трафика, обеспечивая оперативную доставку необходимых данных для АА КРК при сохранении скорости передачи полезных пользовательских данных.

Заключение

В данной статье описаны структура и состав ККА ЗИ ViPNet Quandor, разрабатываемого ОАО «ИнфоТеКС» совместно с МГУ им. М.В. Ломоносова. Обоснован выбор фазового кодирования в используемом протоколе КРК, описан реализуемый способ стабилизации интерференционной картины. Показано, что скорость генерации квантовых ключей должна быть достаточно высокой для применения теоретико-информационно стойкой аутентификации. Также рассмотрено устройство используемого КГСЧ и представлен алгоритм его работы, составленный в процессе разработки АА КРК. Обозначены требования для трафика между АА КРК и ККШ. Отмечено, что для защиты высокоскоростных каналов передачи данных можно не ограничивать скорость служебного трафика.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (проект 03.G25.31.0254).

Литература

1. Shor P. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124–134. – doi: 10.1109/SFCS.1994.365700

2. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М.: Мир, 2006. – 824 с.

3. Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата. – М.: Юрайт, 2017. – 321 с.

4. Bennett C.H. Quantum Cryptography: Public Key Distribution and Coin Tossing / C.H. Bennett, G. Brassard // Proceedings of International Conference on Computers, Systems & Signal Processing. – IEEE, 1984. – PP. 175–179.

5. Балыгин К.А. Активная стабилизация оптической части в волоконной квантовой криптографии / К.А. Балыгин, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2016. – Т. 103, вып. 6. – С. 469–474.

6. Молотков С.Н. О секретности волоконных систем квантовой криптографии без контроля интенсивности квазиоднофотонных когерентных состояний // Письма в ЖЭТФ. – 2015. – Т. 101, вып. 8. – С. 579–585.

7. Управление распределенной интерференцией в однопроходной системе квантовой криптографии / К.А. Балыгин, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2017. – Т. 106, № 2. –С. 108–114.

8. Quantum Key Distribution [Электронный ресурс] // ETSI. – Режим доступа: http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution, свободный (дата обращения: 24.07.18).

9. Abidin A. Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions // Dissertation. – Division of Information Coding, Linkoping University, Linkoping, Swede, 2013.

10. Zhilyaev A.E. On the question of the authentication tag length based on Reed-Solomon codes / A.E. Zhilyaev, E.B. Gurova // Proceedings of Moscow Workshop on Electronic and Networking Technologies. – IEEE, 2018. –

doi: 10.1109/MWENT.2018.8337293. – URL: https://ieeexplore.ieee.org/document/8337293/ (дата обращения: 24.07.18).

11. Quantum Safe Cryptography and Security [Электронный ресурс] // ETSI. – Режим доступа: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf, свободный (дата обращения: 24.07.18).

12. Молотков С.Н. Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов / С.Н. Молотков, К.А. Балыгин, А.Н. Климов, В.И. Зайцев, С.П. Кулик // Письма в ЖЭТФ. – 2017. – Т. 106, № 7. – С. 470–476.

13. Ландау Л.Д. Статистическая физика / Л.Д. Ландау, Е.М. Лифшиц. – М.: Физматлит, 2002. – 1995. – Т. 5, ч. 1. – 616 с.

14. Молотков С.Н. О предельных характеристиках квантовых генераторов случайных чисел при различных группировках фотоотсчетов // Письма в ЖЭТФ. – 2017. – Т. 105, № 6. – С. 374–380.

15. Бабкин В.Ф. Метод универсального кодирования источника независимых сообщений неэкспоненциальной трудоемкости // Проблемы передачи информации. – 1971. – Т. 7, №13. – С. 288–294.

Втюрина Анна Георгиевна
Инженер физического ф-та МГУ им. М.В. Ломоносова
1, Ленинские горы, стр. 2, г. Москва, Россия, 119991
Тел.: +7-904-333-24-56
Эл. почта: ataniru@gmail.com

Елисеев Владимир Леонидович
Канд. техн. наук, руководитель Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 70-59
Эл. почта: EliseevVL@infotecs.ru

Жиляев Андрей Евгеньевич
Исследователь Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7-903-960-05-27, доб. 42-64
Эл. почта: Andrey.zhilyaev@infotecs.ru

Николаева Анастасия Сергеевна
Исследователь Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 45-11
Эл. почта: EliseevVL@infotecs.ru

Сергеев Владимир Николаевич
Вед. исследователь Центра научных исследований и разработок ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 44-95
Эл. почта: Vladimir.Sergeev@infotecs.ru

Уривский Алексей Викторович
Канд. физ.-мат. наук, зам. генерального директора по науке и инновациям ОАО «ИнфоТеКС»
Старый Петровско-Разумовский проезд, д. 1/23, стр. 1,
г. Москва, Россия, 127287
Тел.: +7 (495-7) 37-61-92, доб. 52-49
Эл. почта: Urivskiy@infotecs.ru

Vtyurina A.G., Eliseev V. L., Zhilyaev A.E.,
Nikolaeva A.S., Sergeev V.N., Urivskiy A.V.

On the principal decisions of the practical implementation of the cryptographic devices with quantum key distribution

This article is considering the basic principles of building information security complexes, which allow automatic distribution and usage of quantum keys. Required parts of such complex are described which are needed for the operation of complex as a whole and for quantum key distribution in particular. The authentication scheme for quantum protocol is chosen. The choice of quantum random number generator is justified and algorithm for such generator is developed. The problems of combining encryptors with quantum key distribution devices are indicated and requirements for the logical interface of their interaction are revealed. In addition, authors present results of the analysis of quantum devices' traffic influence on the load of protected channel between encryptors.

Keywords: cryptography, quantum key distribution, quantum random number generator, authentication.
doi: 10.21293/1818-0442-2018-21-2-15-21

References

1. Shor P. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Publ., 1994, P. 124–134, doi: 10.1109/SFCS.1994.365700.

2. Nillsen M., Chang I. *Quantovie vichisleniya I quantovaya informaciya* [Quantum computing and quantum information]. Moscow, Mir Publ., 2006. 824 p.

3. Nesterov S.A. *Informatsionnaya bezopasnost. Uchebnik i praktikum dlya akademicheskogo bakalavriata* [Information security. Textbook and workbook for bachelor students], Moscow, URAIT Publ., 2017. 321 p.

4. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of International Conference on Computers, Systems & Signal Processing. IEEE Publ., 1984, pp. 175–179.

5. Balygin K.A., Klimov A.N., Kulik S.P., Molotkov S.N. Active stabilization of the optical part in fiber optic quantum cryptography. *Jetp Lett.*, 2016, vol. 103, no. 6, pp. 420–424 (In Russ.).

6. Molotkov S.N. On the security of fiber optic quantum cryptography systems without the control of the intensity of quasi-single-photon coherent states. *Jetp Lett*., 2015, vol. 101, no. 8, pp. 579–585 (In Russ.).

7. Balygin K.A., Klimov A.N., Kulik S.P., Molotkov S.N. Control of distributed interference in the one-way quantum cryptography system. *Jetp Lett.*, 2017, vol. 106, no. 2, pp. 120–126 (In Russ.).

8. Quantum Key Distribution. ETSI Publ.. Available at: http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution (accessed 24 July 2018)

9. Abidin A. Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions, Dissertation, Division of Information Coding, Linkoping University, Linkoping, Sweden, 2013.

10. Zhilyaev A.E., Gurova E.B. On the question of the authentication tag length based on Reed-Solomon / Proceedings of Moscow Workshop on Electronic and Networking Technologies, IEEE Publ., 2018, doi: 10.1109/MWENT.2018.8337293. Available at: https://ieeexplore.ieee.org/document/8337293/ (accessed: 24.07.18).

11. Quantum Safe Cryptography and Security. ETSI Publ.. Available at: http://www.etsi.org/images/files/ETSI WhitePapers/QuantumSafeWhitepaper.pdf (accessed 24 July 2018).

12. Balygin K.A., Zaitsev V.I., Klimov A.N. et al. Implementation of a quantum random number generator based on the optimal clustering of photocounts. *Jetp Lett*., 2017, vol. 106, no. 7, pp. 470–476 (In Russ.).

13. Landau L.D., Lifshitz E.M. *Statistical Physics*, *Vol. V, No. 1*, FIZMATLIT Publ., 2002, 616 p. (In Russ.).

14. Molotkov S.N. On the limiting characteristics of quantum random number generators at various clusterings of photocounts. *Jetp Lett.*, 2017, vol. 105, no. 6, pp. 395–401 (In Russ.).

15. Babkin V.F., A Universal Encoding Method with Nonexponential Work Expenditure for a Source of Independent Messages, *Problems Inform. Transmission.,* 1971, vol. 7, no. 4, pp. 288–294.

Anna G. Vtyurina
Engineer, Faculty of Physics,
M.V. Lomonosov State University, Moscow
1, Leninskie Gory, Bld. 2, Moscow, Russia, 119991
Phone: +7-904-333-24-56
Email: ataniru@gmail.com

Vladimir L. Eliseev
Ph.D., Chief of Research and Development Center,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 70-59
Email: EliseevVL@infotecs.ru

Andrey E. Zhilyaev
Researcher, Research and Development Center,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7-903-960-05-27, add. 42-64
Email: Andrey.zhilyaev@infotecs.ru

Anastasia S. Nikolaeva
Researcher, Research and Development Center,
JSC «InfoTeCS», B.Sc. MIPT (SU)
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 45-11
Email: Anastasia.Nikolaeva@infotecs.ru

Vladimir N. Sergeev
Lead Researcher, Research and Development Center,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 44-95
Email: Vladimir.Sergeev@infotecs.ru

Alexey V. Urivskiy
Ph.D., Deputy Director General for Science and Innovation,
JSC «InfoTeCS»
1/23, Staryy Petrovsko-Razumovsky proyezd, Bld. 1,
Moscow, Russia, 127287
Phone: +7 (495-7) 37-61-92, add. 52-49
Email: Urivskiy@infotecs.ru