ОБЗОР

Квантовая криптография и комбинированные схемы коммуникационных сетей на ее основе

А.Ю.Быковский, И.Н.Компанец

Обсуждаются сетевые схемы криптографической защиты данных, сочетающие подходы квантовой криптографии с расширенными методиками компьютерной обработки информации. Использование последних обусловлено наличием ряда нерешенных проблем в существующих системах квантового распределения ключа, а также связано с проектами развития квантовых сетецентрических систем и фотонных сетей, что сопряжено с использованием мультиагентных моделей управления. Рассматриваются разработки на базе протокола Y-00 с кодированием данных квантовыми шумами передающего лазера, а также представлены достижения в области квантово-оптических генераторов случайных чисел. На базе последних возможно создание схем защищенного многозначно-логического кодирования, перспективных для наращивания размерности пространства ключей в методе «одноразового шифроблокнота», для решения задач позиционно-зависимой криптографии и реализации мультиагентных моделей.

Ключевые слова: *квантовое распределение ключа, оптическая связь, фотонная сеть, сетецентрическая система, волоконно-оптическая линия связи, защищенное кодирование, многозначно-логическое защищенное кодирование, мультиагентная система управления сетью.*

Содержание

1. Введение . . . 777
2. Квантовая криптография . . . 778
2.1. Базовые понятия
2.2. Физические принципы КРК
2.3. Разновидности протоколов КРК
2.4. Проблемы создания массовых коммуникационных сетей КРК
2.5. Пример приемопередающего устройства КРК для сетевых ВОЛС
2.6. Многопользовательские полевые сети, реализованные на основе линий КРК
3. Комбинированные сетевые схемы на базе квантовой оптики и расширенного набора методик компьютерной обработки данных . . . 785
3.1. Сетецентрическая система с архитектурой доверенного третьего лица
3.2. Фотонная сеть с мультиагентной системой управления ключами КРК
3.3. Криптографическое кодирование квантовыми шумами передающего лазера
3.4. Возможные схемы атак в квантовых линиях
3.5. Уязвимости компьютерных устройств, обслуживающих сети КРК
4. Направления развития комбинированных схем . . . 793
4.1. КГСЧ для криптографических и компьютерных систем
4.2. «Одноразовый шифроблокнот» на базе КГСЧ и вычислений многозначной логики
4.3. Проблемы, тенденции и задачи развития систем КРК и комбинированных схем
5. Заключение . . . 798
6. Литература . . . 798

1. Введение

Большое внимание к исследованиям в области квантовой криптографии, проводимым уже более 30 лет, определяется остротой проблемы защиты информации в современных коммуникационных сетях, создаваемых на базе волоконно-оптических линий связи (ВОЛС) и схем квантовой оптики. Общее представление о данной тематике можно составить на основании ряда ранних работ [1–5], обзоров [6, 7, 31–35, 42, 56–70] и книг [197–204], а также учебно-популярных изданий [205, 206].

Фактически под термином «квантовая криптография» понимают [2, 6] метод конфиденциального квантового распределения криптографических ключей (КРК) (QKD – Quantum Key Distribution) между участниками сети, когда линия или сеть КРК решает задачу доверенного «курьера» по доставке секретных ключей абонентам.

В 2016 г. в журнале Journal of Optics [7] была опубликована «дорожная карта» развития систем оптической

А.Ю.Быковский, И.Н.Компанец. Физический институт им. П.Н.Лебедева РАН, Россия, 119991 Москва, Ленинский просп., 53; e-mail: ayubykov@sci.lebedev.ru

Поступила в редакцию 16 мая 2018 г., после доработки – 25 июля 2018 г.

связи, где квантовая криптография была включена ведущими экспертами в число 17 наиболее актуальных направлений. Прорабатывается вопрос об использовании схем КРК в сетецентрических системах [8–10], являющихся глобальными компьютерными и коммуникационными сетями, обслуживающими критическую инфраструктуру, военную технику и устройства различного назначения, включая беспилотные. Более того, схемы КРК предполагается использовать в фотонных (чисто оптических) сетях [11–14]. Интересные эксперименты проведены недавно по реализации КРК между спутниками и наземными станциями [15–17]. Продолжаются зарубежные исследования и начаты российские эксперименты с полевыми (развернутыми на местности) многопользовательскими (многоузловыми и разветвленными) сетями КРК [18–28].

Однако практическое внедрение метода КРК в массовые коммуникационные сети оказалось не столь быстрым, как ожидалось в начале 2000-х годов [29, 30], и столкнулось с рядом проблем [6, 31–35], значительная часть которых не решена до настоящего времени. В 2016 г. был опубликован официальный документ (white paper) Национального центра кибернетической безопасности Великобритании (NCSC) [36], в котором сформулирован ряд недостатков существующих систем КРК и задано направление приоритетного развития традиционных криптографических систем в рамках так называемой постквантовой криптографии [37, 38].

Как следует из данных [39, 40], работа над европейскими коммерческими стандартами для оборудования КРК до сих пор не завершена. Также показательным является тот факт, что Национальный институт стандартов и технологий США (NIST), являющийся головным разработчиком несекретных стандартов в области связи и криптографии, до настоящего времени публикует методические материалы по КРК на своем сайте [41] лишь в рамках проекта «квантовые коммуникации» и не включает их в направление «кибербезопасность». На сайте NIST из более чем десяти известных протоколов КРК представлен лишь BB84 [2–4, 42]. Это свидетельствует о том, что NIST к настоящему времени так и не сформировал открытого проекта по массовому внедрению метода КРК, оставив его в статусе перспективного защищенного средства связи для сети квантовых вычислительных устройств. При этом в 2016 г. NIST запустил новый проект по постквантовой, или квантово-устойчивой криптографии [37, 38], направленный на создание алгоритмов шифрования, стойких к «взлому» с помощью как обычных, так и квантовых компьютеров. Анализ патентов в сфере КРК [43] также выявил задержки с выбором приоритетов рядом основных разработчиков.

Следует также отметить опубликованные в популярных интернет-ресурсах скептические высказывания такого авторитетного специалиста в области компьютерной безопасности, как Б.Шнайер [44], комментируемые обозревателем одного из компьютерных сайтов [45, 46].

Не решенные до настоящего времени проблемы препятствуют широкому внедрению схем КРК в массовые коммуникационные сети и усложняют процедуры управления совокупными сетевыми криптографическими средствами. Это вынуждает внедрять мультиагентные методы [47], облегчающие имитацию интеллектуальных функций человека в системах управления, а также мотивирует разработку комбинированных сетевых схем, сочетающих квантовую оптику с усложненными методиками компьютерной обработки данных [8–12, 48–51].

Приведенные выше факты послужили мотивацией к написанию данного обзора, цель которого заключается:

1) в анализе факторов, задерживающих давно обещанное внедрение схем КРК в массовые телекоммуникационные сети [29, 30];

2) в анализе причин, вызвавших активную разработку криптографических систем на базе протокола Y-00 [48–51], в котором квантовые шумы передающего лазера и традиционные методы шифрования используются для двойного кодирования сигналов, передаваемых интенсивными лазерными импульсами;

3) в анализе мотивации разработки сетецентрических систем и фотонных сетей [8–14], в которых схемы КРК интегрированы в мультиагентные системы управления криптографическими средствами;

4) в выявлении тенденций развития квантовых генераторов случайных чисел (КГСЧ) [52, 53] и перспектив создания на их основе схем защищенного многозначнологического кодирования (МЗЛК) [54, 55] высокой размерности.

Для краткости, по ряду вопросов ссылки даны не на первоисточники, а на обзоры и статьи, которые лучше соответствуют целям настоящей работы.

2. Квантовая криптография

2.1. Базовые понятия

Главной задачей линии КРК [2–4, 6, 32–35, 42, 56–61] является конфиденциальное распределение общего криптографического ключа между двумя абонентами, обычно обозначаемыми как Алиса и Боб, которые сохраняют этот ключ в тайне от злоумышленника Евы. Набор несанкционированных действий Евы, позволяющих ей частично или полностью узнать секретный ключ, распределяемый между Алисой и Бобом [4, 31, 32, 56, 57, 62], рассматривается в схемах КРК как атака. При этом особенности схем, процедур и оборудования, облегчающие проведение атак и получение информации злоумышленником, называют уязвимостями.

Задача защиты квантовой линии от злоумышленников затрагивает столь большое количество вопросов квантовой оптики, компьютерной обработки данных и защиты информации, что ни один из опубликованных обзоров [6, 7, 31–35, 42, 56–70] не охватывает всех аспектов этой задачи. Поскольку недавний обзор 2016 г. [57] был целенаправленно посвящен структуре и взаимосвязи средств, используемых в квантовой линии для ее защиты от злоумышленников, эти вопросы лишь кратко обсуждаются в настоящей работе.

Как и для любой криптографической системы, базовыми понятиями для схем КРК являются понятия конфиденциальности, целостности передаваемых данных и аутентификации (проверки подлинности) абонентов, обсуждаемые в литературе по информационной безопасности компьютерных систем [71, 72] и в обзорах [6, 56, 57, 70]. Таким же базовым понятием является теорема о невозможности точного клонирования квантовых состояний, обсуждаемая в [6, 42, 57–59]. Способы построения измерительных базисов в линиях КРК описаны подробно в [6, 31, 42] и кратко изложены в [57, 59, 63, 64].

Протоколы КРК, являющиеся связующим звеном для всех компонентов системы защиты квантовой линии, обсуждаются в той или иной мере в обзорах [6, 7, 31–35, 42, 58–66, 69]. Самый востребованный протокол BB84 подробно описан в [4, 6, 31, 42, 63], а краткое изложение его и ряда других наиболее известных протоколов представлено в [33, 58, 60, 64, 68].

Принципы работы BB84, необходимые для понимания ее аспектов, кратко изложены далее в разд.2.1. Там же обсуждается метод обнаружения злоумышленника, производящего измерения квантовых состояний в линии КРК [6, 31, 42, 57, 59], что требует вычисления коэффициента ошибочных квантовых битов QBER (Quantum Bit Error Rate).

Обсуждение возможных схем атак на компоненты линии КРК и мер противодействия им вынесено в разд.3.4, чтобы подчеркнуть их отличие от методов защиты информации в компьютерных сетях, представленных в разд.3.5. Ранее схемы атак подробно рассматривались в обзорах [31, 56, 57, 60, 62].

Взаимосвязь протокола BB84 со схемами сетевых квантовых вычислений, для защиты которых в перспективе необходимы схемы КРК, подробно обсуждается в обзорной работе [42], опубликованной NIST в 2002 г.

2.2. Физические принципы КРК

В результате специальной процедуры пересылки от Алисы к Бобу квантовых состояний, передаваемых с помощью одиночных фотонов либо ослабленных лазерных импульсов (с одним и менее фотонов на импульс), у обоих абонентов формируются две одинаковые случайные последовательности битов, называемые «сырым» ключом. Сырой ключ дополнительно обрабатывают с помощью статистических методов, используя процедуры просеивания, коррекции ошибок и усиления секретности [6, 28, 31, 42, 59, 73]. Итоговый ключ используют далее в криптографическом протоколе «одноразового шифроблокнота» – ОШБ (one-time pad) [6, 42, 56, 57, 72, 74], который гарантированно является наиболее защищенным видом кодирования и реализует совершенный (т.е. невзламываемый) код Вернама, для которого возможен лишь прямой перебор ключей – атака методом грубой силы. Ключи можно «расходовать» более экономно, применяя их в менее защищенных методиках шифрования, например в AES (Advanced Encryption Standard – симметричный алгоритм блочного шифрования, принятый в качестве стандарта в США) [41, 56, 72].

Физический принцип работы схем КРК базируется на теореме о невозможности клонирования (или точного копирования) квантовых состояний [75], основанной на ряде постулатов квантовой механики [42]. Указанная теорема часто интерпретируется как невозможность неразрушающих измерений, вследствие чего измерения состояний кубитов (двухуровневой квантовой системы), скрытно выполняемые злоумышленником Евой в квантовом канале, будут приводить к увеличению числа ошибок в случайной битовой последовательности ключа, нарабатываемого Алисой и Бобом. Происходящее при этом увеличение коэффициента ошибочных квантовых битов QBER [6, 31, 42, 59, 76–81], обсуждаемое ниже, позволяет установить факт подслушивания.

Неизбежные потери части фотонов в реальном атмосферном канале или в ВОЛС вынудили признать неэффективной [31] схему прямой передачи секретных сообщений с помощью одиночных фотонов, которая обсуждалась в ряде ранних работ по КРК. Соответственно, в любом современном проекте схема КРК интегрирована с обычными сетевыми средствами криптографической защиты.

Процедура формирования секретного ключа у пары абонентов (Алиса и Боб) называется протоколом КРК [2–4, 6, 31, 42, 56–60, 62, 63]. Первый и наиболее востребованный протокол КРК, названный в [2] BB84, изображен на рис.1 в виде схемы с поляризационным кодированием света из работы [65]. В отличие от состояния обычного бита, состояние кубита описывается суперпозицией соответствующих волновых функций [2–4, 6, 31, 42, 59]. Для построения схемы КРК необходимо использовать два канала связи: квантово-оптический (прямая черная линия на рис.1), выполненный в виде секции ВОЛС или атмосферной лазерной линии, а также открытый неквантовый канал (на рисунке не показан), реализуемый с помощью той же ВОЛС или отдельной линии связи. В случае использования для регистрации слабых оптических сигналов электронных схем совпадения потребуется обязательная синхронизация квантового и неквантового каналов [57].

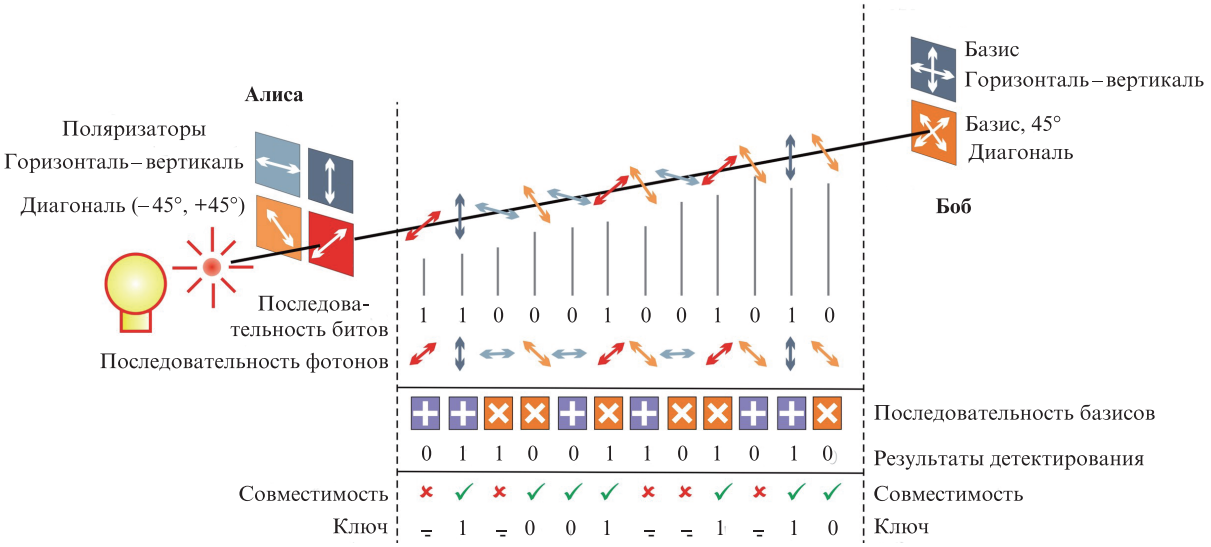


Рис.1. Схема КРК по протоколу BB84 [65].

Отправитель Алиса и получатель Боб используют два ортогональных базиса (две пары осей поляризатора), позволяющих измерять четыре различных состояния поляризации. Первый (прямой) базис задает значения 0 и 1 посредством горизонтальной (↔) и вертикальной (↕) осей поляризатора. Второй (диагональный) базис для передачи 0 и 1 использует диагональные оси –45° (↘) и +45° (↗).

В процессе распределения ключа Алиса отправляет по квантовому каналу одиночные фотоны, каждый из которых может иметь четыре возможных (↔, ↕, ↘, ↗) значения поляризации, выбираемых Алисой с помощью своего генератора случайных чисел. Сгенерированный ею случайный набор из 0 и 1, показанный на рис.1 в строке «последовательность битов», закодирован набором поляризаций фотонов, представленных в строке «последовательность фотонов». Боб измеряет поляризацию получаемых фотонов, случайно выбирая с помощью своего генератора случайных чисел набор горизонтальных или диагональных базисов, обозначенных символами (+ и ×) в строке «последовательность базисов». Завершив цикл приема, Боб отправляет Алисе по неквантовому каналу данную последовательность выбранных им базисов, а Алиса в ответ сообщает Бобу использованную ею последовательность базисов. Затем они отбрасывают те результаты измерений (обозначены крестиками в строке «совместимость»), для которых использованные ими базисы не совпали. При этом сырой ключ укорачивается и далее называется просеянным ключом, состоящим из оставшихся 0 и 1, показанных в строке «ключ».

Просеянный ключ содержит некоторое число ошибок (несовпадений битов у Алисы и Боба), связанных с неснижаемыми оптическими потерями в канале, шумами фотодетекторов, техническими сбоями и возможным вмешательством злоумышленника. Поэтому далее требуется использовать процедуры статистической обработки, необходимые для обнаружения злоумышленника, коррекции ошибок и усиления секретности ключа [4, 6, 31, 42, 60, 73, 82]. Попытки злоумышленника Евы «подслушать» передаваемые данные в квантовой линии сопровождаются процессом разрушающих измерений кубитов и увеличением общего количества ошибок в просеянном ключе [2–4, 6, 31, 73, 82]. В связи с этим факт несанкционированного подслушивания может быть обнаружен с помощью проверки числа совпадений битов у Алисы и Боба в случайной выборке из просеянного ключа. При вмешательстве злоумышленника в работу квантовой линии Алиса и Боб обнаружат увеличение числа ошибок по сравнению с уровнем, наблюдаемым в отсутствие Евы.

Описанная выше процедура обнаружения факта незаконного прослушивания квантовой линии основана на вычислении коэффициента QBER и обсуждается, например, в обзорах [6, 31, 57, 63]. Коэффициент QBER определяет относительную долю ошибочных битов в полученной последовательности и оценивается как отношение вероятности регистрации ошибочных битов к вероятности регистрации их общего числа в пересчете на один передающий импульс.

Из теоретической модели, представленной в [76], следует, что, при использовании классических алгоритмов статистической обработки в процедурах коррекции ошибок и усиления секретности ключа, увеличение QBER приводит к нелинейному уменьшению длины получаемого итогового ключа. Из ряда других работ, подтверждающих такой же характер зависимости, можно указать на более позднюю работу [77], где был проведен подробный анализ экспериментальных данных, полученных для протокола BB84, который был реализован в линии КРК со схемой спектрального уплотнения каналов (мультиплексирования) WDM. В этой работе сделаны теоретические оценки скорости наработки итогового ключа и коэффициента QBER. В том числе было наглядно показано, что одна часть битов просеянного ключа, наработанного в единицу времени, отбрасывалась (расходовалась) во время процедуры коррекции ошибок, а другая часть битов затрачивалась на процедуру усиления секретности ключа. При этом каждая из долей просеянного ключа, использованных при его статистической обработке, нелинейно возрастала с увеличением QBER. В работе [77] в процедуре коррекции ошибок использовался известный алгоритм CASCADE, а процедура усиления секретности ключа была основана на вычислениях хэш-функций, рассчитываемых с помощью матриц Теплица.

Из представленных выше примеров следует, что превышение определенной предельной величины QBER [6, 63, 76–81, 83] резко снижает скорость наработки итогового ключа и заставляет абонентов прерывать сеанс связи или переходить на другой канал [57]. При этом количество регистрируемых ошибочных битов в квантовом канале КРК существенно зависит от используемого протокола и параметров конкретной линии, в связи с чем предельная величина QBER рассчитывается для конкретного протокола [76–81, 84–89].

В [79] для протокола BB84 была получена предельная величина QBER, составившая ∼11% и вычисленная с помощью понятия энтропии в рамках теории информации Шеннона. При этом теоретическая модель, учитывавшая возможность выполнения Евой только так называемых индивидуальных атак (см. разд.3.4), позволяла оценивать предельную вероятность знания злоумышленником определенной доли ключа на различных стадиях его статистической обработки. Предельная величина QBER, рассчитанная для когерентных атак на протокол BB84 в [6], также составила ∼11%. Как подчеркнуто в обзоре [57], величины QBER, близкие к 11%, были получены для BB84 в целом ряде публикаций, но используемые в них модели в большинстве случаев не учитывали реальные характеристики лазерных источников, фотодетекторов и оптоволокна. Поэтому производители коммерческих установок КРК Clavis2 (Id Quantique, Швейцария) на практике рекомендовали пользователям работать с предельными величинами QBER, равными ∼8%.

Значительное внимание было уделено вопросу о взаимосвязи величины коэффициента QBER с максимальной длиной квантового канала [6, 31, 32, 76–81]. В работе [79] отмечено, что в большинстве публикаций коэффициент QBER рассматривали как постоянную величину, тогда как авторы указанной работы показали экспоненциальный рост QBER при увеличении длины квантового канала. Этот результат был получен для разновидности протокола BB84 с состояниями-ловушками (обсуждаются в разд.2.2). Подобный характер зависимости коэффициента QBER от длины квантового канала был также обоснован теоретически в работе [80] для протокола BB84 с поляризационным кодированием кубитов в квантовой линии, использующей схему спектрального уплотнения каналов (WDM). Однако в этой же работе было показано, что для схемы с временным уплотнением каналов (TDM) режим с линейным ростом QBER потенциально возможен при уве-

личении длины линии (общая длина ВОЛС не более 200 км). Увеличение длины квантовой линии также может быть ограничено негативным влиянием перекрестных помех, возникающих при передаче квантовых сигналов по одной ВОЛС вместе с обычным потоком данных [80].

В [81, 83] было показано, что величина QBER зависит не только от оптических потерь в линии, шумов и ошибок фотодетектора в конкретной схеме КРК, но также от внешних неконтролируемых воздействий и качества системы стабилизации параметров линии КРК. Например, в [81] время непрерывной наработки итогового ключа составляло около 30 мин. Следовательно, величина QBER в линии КРК должна постоянно и тщательно контролироваться ее системой управления.

Расчеты скорости наработки итогового ключа и предельной величины QBER тесно связаны с теоретическим обоснованием уровня криптостойкости протоколов КРК [6, 31, 57]. Это требует создания квантово-механической модели, описывающей действия Алисы, Боба и Евы, а также оценивающей, насколько успешно используемые процедуры коррекции ошибок и усиления секретности ключа позволяют свести к пренебрежимо малой величине ту часть ключа, которая может стать известной злоумышленнику [6, 31–33, 57, 59, 78–81, 86, 87]. С этой целью в моделях криптостойкости, обсуждаемых, например, в [33, 78], были получены выражения для оценки параметра ε, характеризующего меру отклонения распределения ключа от случайного и определяющего вероятность того, что злоумышленник знает определенную часть ключа после завершения процедур протокола.

Отдельная проблема заключается в корректном описании реального уровня шума и оптических потерь в оптоволокне, в учете вероятности ложных срабатываний однофотонных фотоприемников, а также в учете неоптимальной юстировки модуляторов в оптической схеме [57, 76–81, 87–89]. Следует также учитывать, что для одного и того же протокола могут быть теоретически обоснованы несколько разных моделей криптостойкости [6, 89].

При построении теоретических моделей протоколов КРК разработчики, в первую очередь, стараются обосновать безусловную (unconditional) криптостойкость протокола, не зависящую от вычислительной мощности злоумышленника [6, 31, 32, 84, 88]. В обзорах [32, 57] особое внимание было уделено такому важному вопросу теоретического анализа криптостойкости, как учет конечной длины реального ключа в моделях, исходно построенных на предположении о бесконечной длине ключа [84, 90]. Проводятся исследования и других сложных вопросов, например корректности оценок криптостойкости, получаемых при описании процесса измерения сигнала с помощью проектора (оператора) в гильбертовом пространстве малой размерности [91]. Тем не менее пока не сформирован достаточно всеобъемлющий и однозначно интерпретируемый набор методов теоретической оценки криптостойкости схем КРК, на необходимость создания которого указывал автор [32].

2.3. Разновидности протоколов КРК

Наиболее востребованным до настоящего времени остается протокол BB84 (1984 г.) [2–4], помимо которого известны более десяти других протоколов КРК, обсуждавшихся, например, в [6, 31, 34, 35, 60, 64, 68]. Этот протокол в вариантах с фазовым и поляризационным кодированиями кубитов использовался в большинстве проектов полевых сетей КРК, что видно из приведенной в разд.2.5 табл.1. При этом наиболее распространенной версией BB84 является вариант этого протокола, дополнительно использующий состояния-ловушки (decoy-state) [92]. В данном случае к передаваемой серии ослабленных лазерных импульсов добавляют ложные импульсы, содержащие случайно заданное число фотонов (обычно ~1 фотон/имп.). Это позволяет исказить случайным образом статистику числа фотонов в квантовом канале, необходимую злоумышленнику для выполнения атак с использованием светоделительных элементов [31]. Для такого протокола теоретически обоснована большая дальность гарантированно защищенного КРК [33].

Протоколы BB92 (1992 г.) и SSP (1999 г.) отличаются от BB84 прежде всего числом использованных базисов и применением для кодирования кубитов двух и шести квантовых состояний соответственно [31]. В [64] отмечено, что протокол SARG04 (2004 г.) отличается от BB84 в основном процедурой кодирования, разработанной для противодействия атакам с разделением по числу фотонов. Там же кратко комментируются отличия процедур, используемых протоколами KMB09 (2009 г.) и S13 (2013 г.) в квантовом и не квантовом каналах, от аналогичных процедур BB84.

В широко известном дифференциально-фазовом протоколе DPS (Differential Phase Shift, 2003 г.), подробно анализируемом в [93], информация о ключе кодируется в относительную разность фаз когерентных состояний в каждой соседней посылке. Лазер Алисы работает в режиме синхронизации мод и выдает серии сфазированных импульсов. Модулятор формирует последовательность ослабленных лазерных импульсов одинаковой интенсивности, разделенных одинаковыми временными интервалами. При этом все импульсы в разных посылках взаимно когерентны, т. е. частотная «набивка» имеет одинаковую фазу. Далее фазовый модулятор либо изменяет фазу, $|\alpha\rangle \rightarrow |-\alpha\rangle$, либо оставляет ее неизменной, в зависимости от необходимости передать 0 или 1. Для приема сигналов Боб использует разбалансированный интерферометр Маха–Цендера.

Так называемый когерентный протокол COW (Coherent One Way, 2004 г.), подробно обсуждаемый в [19, 94], возник на базе DPS и использует амплитудную модуляцию последовательностей лазерных импульсов одинаковой интенсивности, разделенных одинаковыми временными интервалами и взаимно когерентных. При этом 0 кодируют последовательной передачей пары импульсов «уровень вакуума–когерентное состояние», а 1 передают отправкой пары импульсов «когерентное состояние–уровень вакуума». Регистрация сигналов также производится разбалансированным интерферометром Маха–Цендера.

Основным минусом протоколов DPS и COW считают недостаточный уровень теоретического обоснования их криптостойкости [57].

В последние годы значительное внимание также уделяется так называемым схемам КРК, не зависящим от измерительных устройств и обозначаемым DI-QKD или MDI-QKD (Device-Independent или Measurement-Device-Independent) [95, 96].

С точки зрения оригинальности принципа действия выделяется протокол E91 (1991 г.), в литературе часто обозначаемый EPR и основанный на свойствах «запутан-

ных» состояний квантовых частиц, предложенных Эйнштейном, Подольским и Розеном [97]. В этом протоколе, основанном на проверке выполнения соотношений типа неравенства Белла [98,99], запутанную фотонную пару создают методом спонтанного параметрического рассеяния света. В связи с развитием космических систем КРК [34] интерес к данному протоколу сохраняется и в настоящее время.

Достаточно подробно исследованы также схемы КРК с непрерывными переменными (CV) и кодированием в квадратурных амплитудах мод квантованного электромагнитного поля [100].

2.4. Проблемы, затрудняющие создание массовых коммуникационных сетей КРК

Известно, что размер кодируемого массива данных для метода «одноразового шифроблокнота» не может превышать суммарной длины использованных случайных одноразовых ключей [72, 74], т. е. скорость наработки ключа определяет размер массива, передаваемого в единицу времени. Поскольку уже созданы ВОЛС со скоростью передачи 100 Гбит/с на один частотный канал [35, 101] и в полевых условиях опробованы сети с суммарной пропускной способностью 54.2 Тбит/с [102], то для потокового шифрования методом «одноразового шифроблокнота» требуются скорости КРК на уровне 100 Гбит/с и более. Однако достигнутые в настоящее время скорости КРК составляют лишь ~1 Мбит/с при длине квантовой линии до 50 км (см., напр., [11, 35, 103]). При этом для полевой сети ВОЛС внешние факторы дополнительно снижают скорость КРК. Например, в [24] для ВОЛС на катушке она превышала 1 Мбит/с в лабораторных условиях, но в полевых условиях снижалась до 304 кбит/с.

С другой стороны, увеличение длины квантовой линии более 80 – 100 км [33, 76 – 81, 103] приводило к резкому снижению скорости гарантированно защищенного КРК, что теоретически обосновано, например, в [78, 84, 104] и обусловлено потерями в ВОЛС и характеристиками современных однофотонных приемников. В частности, длина квантового канала 80 км соответствовала наибольшей скорости КРК порядка 100 кбит/с [103], но длина ВОЛС 100 км позволила получить скорость КРК лишь ~10 кбит/с [105]. А для ВОЛС с ультранизким уровнем потерь 0.16 дБ/км, обеспечившим рекордную дальность КРК в 307 км, скорость КРК составила всего 3.18 бит/с [106].

Следует подчеркнуть, что для корректного сравнения скоростей КРК необходимо учитывать не только уровень оптических потерь в волокне (у большинства авторов это 0.2 дБ/км), но и особенности алгоритма обработки ключа, а также величину расчетного параметра ε, характеризующего степень отклонения ключа от идеальной статистической модели и уровень его криптостойкости [33, 35, 106]. Однако некоторые авторы для простоты скорость КРК в ВОЛС оценивают в ~1 Мбит/с, а дальность распределения квантовых ключей – в 150 – 200 км.

Таким образом, достигнутый уровень скоростей КРК позволяет использовать квантовые ключи для шифрования методом «одноразового шифроблокнота» лишь для «нишевых» задач, когда возможны попытки считывания данных из канала связи, но высокая производительность не требуется.

Кроме того, для увеличения дальности нынешних схем КРК необходимо использовать ретрансляторы [6, 10, 11, 19, 21, 24, 31, 35, 56]. Поскольку практически работоспособные ретрансляторы с квантовой памятью для кубитов еще не созданы, то экспериментальные разработки сетей КРК базируются на так называемых доверенных ретрансляторах (см., напр., [8 – 12, 18 – 27]), создаваемых на базе обычных компьютеров. Другая возможность заключается в создании космических систем КРК [6, 34], когда в условиях вакуума легче, чем в ВОЛС, реализовать КРК на больших расстояниях. Именно этим объясняется давно ожидавшийся всплеск активности в области разработки космических схем КРК [15 – 17].

Еще одна нерешенная проблема связана с реализацией эффективных схем объединения одиночных линий КРК в разветвленную многопользовательскую сеть [8, 9, 11 – 13, 18 – 28, 69]. Квантовые схемы разветвителей пока не реализованы, а использование в этих целях пассивных оптических переключателей и разветвителей [107, 108], а также оптических мультиплексоров [109, 110] приводит к неприемлемо большому росту оптических потерь и шумов и, кроме того, оказывается технически сложным. С другой стороны, использование чисто компьютерных доверенных ретрансляторов на базе стандарта AES [8 – 12, 18 – 28] для разветвления сети КРК сводит в итоге ее уровень защищенности к уровню защищенности обычных компьютерных систем. Поэтому в настоящее время более интересной представляется методика на основе пассивных волоконных разветвителей [107, 108].

К техническим сложностям создания схем КРК следует отнести проблемы снижения потерь ВОЛС до уровня менее 0.16 дБ/км, а также совершенствования оптических компонентов и схем стабилизации температуры, фазы и поляризации света [8 – 13, 83]. Требуют дополнительной проверки результаты экспериментов [83], при проведении которых авторы исследовали взаимосвязь числа разъемных и сварных соединений оптоволокна с величиной QBER. При этом квантовая линия с одномодовым волокном TELECOM состояла из постоянно задействованной секции, необходимой для создания временных задержек и синхронизации, а также из секции длиной 6.5 км, последовательно с которой с помощью стандартных разъемов FC/PC подключали до пяти-семи дополнительных секций длиной от 1 до 72 м. Такую линию соединяли с двухпроходной установкой КРК Clavis II (IdQuantique) с фазовым кодированием кубитов. Для каждого набора дополнительно подсоединенных секций набирали статистику в течение 20 – 50 ч, а обработку полученных сырых ключей длиной 512 бит каждый проводили с использованием методов кластерного анализа данных. Основной результат заключался в том, что уже при подключении пяти дополнительных секций длиной 2 м каждая рост оптических потерь на разъемных соединениях увеличивал коэффициент QBER до значений, превышающих 11%, что не обеспечивало защиту от прослушивания. Исследования ВОЛС со сварными соединениями секций приводили к аналогичным результатам.

2.5. Пример приемопередающего устройства КРК для сетевых ВОЛС

В качестве успешного примера реализации варианта протокола BB84 с состояниями-ловушками (decoy-state), на рис.2 показана схема модуля КРК с фазовым кодированием кубитов, созданная Toshiba Research Group (Великобритания) в рамках проекта Tokyo QKD network

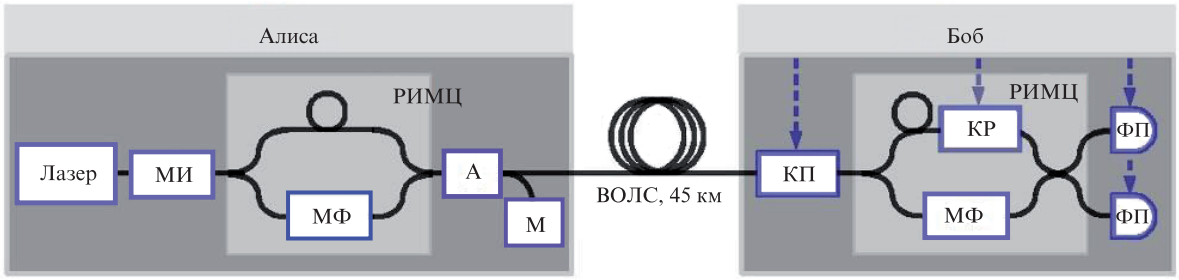


Рис.2. Схема приемопередающего устройства КРК, использующего фазовое кодирование кубитов и протокол BB84 с состояниями-ловушками [24].

[24]. Данная разработка в условиях полевой сети показала рекордную скорость распределения полностью обработанного ключа в 304 кбит/с для секции ВОЛС длиной 45 км, несмотря на сравнительно высокий уровень оптических потерь (14.5 дБ), обусловленный частичной прокладкой оптоволокна в воздухе.

Передающий модуль Алисы содержал лазер с распределенной обратной связью (DFB), генерировавший импульсы излучения на $\lambda = 1550$ нм длительностью 50 пс с частотой следования 1 ГГц. Модулятор интенсивности (МИ) формировал три усредненных уровня интенсивности: 0.5 фотон/имп. для полезного сигнала, а также уровни 0.1 и 0.0007 фотон/имп. для состояний-ловушек. Кодирование полезной информации осуществлялось модулятором фазы (МФ) в одном из плеч разбалансированного интерферометра Маха–Цендера (РИМЦ). Уровень сигнала в схеме контролировался аттенюатором А и системой мониторинга М.

В приемном модуле Боба использовался контроллер автоподстройки поляризации КП и второй РИМЦ, в одном из плеч которого размещался модулятор фазы МФ, а в другом – контроллер растяжения/длины волокна (стретчер) (КР). Фотоприемниками (ФП) служили охлаждаемые до –30 °С лавинные фотодиоды (ЛФД) на основе InGaAs с саморазностной (self-differencing) схемой стробирования на частоте 1 ГГц, использованной для компенсации влияния постпульсаций и паразитных емкостных элементов [111]. При этом эффективность регистрации составила 19%, а частота темновых отсчетов – около 10 кГц.

Авторы [24] объяснили достижение рекордных скоростей в полевых условиях следующими новшествами:

– учетом скорости срабатывания ЛФД в качестве параметра обратной связи для цепи задержки сигналов стробирования;

– учетом величины QBER в контуре волоконного стретчера, корректирующего растягивающее усилие и минимизирующего негативный эффект от практической работы с ключом конечной длины, считающейся бесконечной в теоретических моделях;

– снижением дрейфа параметров и увеличением времени стабильной работы схемы до десятков минут, что было достигнуто за счет тщательной проработки схемы синхронизации и использования для квантового и классического каналов оптоволокна из одного жгута;

– уменьшением временного окна стробируемых фотоприемников до 100 пс;

– использованием усовершенствованных процедур просеивания случайного ключа, коррекции ошибок в нем и усиления его секретности, основанных на вычислениях матриц Теплица с размером блока в несколько сотен килобит на многоядерных PC.

2.6. Многопользовательские полевые сети, реализованные на основе линий КРК

На базе линий КРК типа «точка–точка», обслуживающих пару абонентов, был реализован ряд проектов полевых многопользовательских сетей КРК [18–27], в которых ВОЛС и атмосферные линии размещались на местности, подвергаясь максимальному воздействию внешней среды. В Российской Федерации также было запущено несколько проектов линий и полевых сетей КРК (см., напр., [26, 28]).

Основные параметры наиболее характерных проектов полевых многопользовательских (многоузловых) сетей представлены в табл.1. Из приведенных в ней проектов КРК наиболее масштабными являются проекты в [19, 24, 25], объединяющие линии КРК различных разработчиков. К наиболее популярным относится протокол BB84 с состояниями-ловушками, реализуемый и для поляризационного и для фазового кодирования. Полученные различными авторами величины QBER в рабочем диапазоне 0–11% характеризуют неснижаемый уровень шума и потерь в реализованных ими квантовых каналах. Этот уровень, как видно из табл.1, напрямую не коррелирует со скоростью наработки итогового ключа и дальностью его передачи.

В табл.1 представлены проекты сетей КРК, в каждом из которых было реализовано 3 –10 сетевых узлов. Расстояния между ними варьировались от 12 до 85 км, а скорость распределения ключей составляла 0.9–304 кбит/с. При этом авторы [23] оценивали скорость ~1 кбит/с как потенциально достаточную для обслуживания криптографических протоколов стандарта AES с длиной ключа 256 бит в сети и скоростью передачи данных 2.4 Гбит/с.

Поскольку квантовые ретрансляторы [6, 33, 35, 56, 57] пока не созданы практически, то в проектах сетей КРК, представленных в табл.1, в различных вариантах скомбинированы компьютерные доверенные узлы и оптические переключатели.

Например, в [23] (см. табл.1) дан пример интеграции в существующую городскую сеть квантовых ВОЛС на двух уровнях: 1) высокоскоростных опорных (backbone) линий и сетевых сегментов (называемых также магистральными, основными или скелетными), решающих задачи межсоединений «все-со-всеми», и 2) сетей доступа (access network), доставляющих контент от основных магистралей к конечным пользователям.

Серьезные усилия, предпринимаемые в Китае по освоению сетей КРК, демонстрируют работы [21, 25] (см. табл.1). В [21] описана сеть из пяти узлов с топологией «звезда» и поляризационным кодированием кубитов в одномодовом волокне, где доверенные ретрансляторы комбинируются с оптическими переключателями и мето-

Табл.1. Параметры полевых многоузловых сетей.

Источник/ год	Страна/проект	Местоположение/ участники	Число узлов	Назначение/длина линии/уровень потерь	Скорость КРК/QBER	Протокол КРК/ тип кодирования
[18]/2005	США/Quantum Network	Кембридж/DARPA, BBN, Гарвардский и Бостонский университеты	10	Городская сеть/ 10.2 км/5.1 дБ	500 бит·с$^{-1}$ (полевые условия)	BB84, SARG04/ф.к.
				Городская сеть/ 19.6 км/11.5 дБ	10 бит·с$^{-1}$ (лабораторные условия)/н.д.	
[19]/2009	Австрия/ SECOQC	Вена/Siemens,59 университетов и компаний	6	6.2 км/2.8 дБ	8 кбит·с$^{-1}$/н.д.	CW, г.д.
				16 км/н.д.	2.5 кбит·с$^{-1}$/3.5%	EPR
				19 км/н.д.	н.д.	BB84, SARG04/ф.к.
				22 км	н.д.	н.д.
				25 км/6 дБ	~1 кбит·с$^{-1}$/<2.8%	н.д.
				33 км	3.1 кбит·с$^{-1}$/2.6%	Decoy-st./ф.к.
				85 км	н.д.	COW/в.к.
[20]/2009	США/ATD-net	Колледж-Парк/ Лаборатория телекоммуникационных наук	3	25 км	1090 бит·с$^{-1}$/5.9%	BB84/ф.к.
				10 км (на катушке)	н.д.	
				5 м	н.д.	
[21]/2010	Китай/проект без названия	Хэфэй, Ван ан, Ванкси/USTC	5	4 городские линии/ от 8.4 км/2.65 дБ до 10 км/2.82 дБ	>1.2 кбит·с$^{-1}$/2% (среднее значение)	Decoy-st./п.к.
				1 межгородская линия/60 км/17 дБ	4.5 кбит·с$^{-1}$/1.13%	
[22]/2010	ЮАР/ QuantumCity	Дурбан/ Ква-Зулу-Наталь	4	2.6–27 км	891 бит·с$^{-1}$/1.7%	BB84/ф.к. в схеме plug&play
[23]/2011	Испания/проект без названия	Мадрид/ Политехнический университет	3	Опорная городская линия/6 км	0.5 кбит·с$^{-1}$/н.д.	Decoy-st./ф.к.
				10 км	100 бит·с$^{-1}$/н.д.	
				Городская сеть доступа/1 км	~200 бит·с$^{-1}$/н.д.	
				3.5 км	20 бит·с$^{-1}$/н.д.	
[24]/2011	Япония/QKD Network	Токио/NICT, 9 организаций из Японии и ЕС	6	1 км/1 дБ	0.25 кбит·с$^{-1}$/5%–7%	EPR (BBM92)
				13 км/11 дБ	400 бит·с$^{-1}$/2%	SARG04/ф./к.
				24 км/13 дБ	2 кбит·с$^{-1}$/4.5%	Decoy-st./ф.к.
				45 км/14.5 дБ	81.7 кбит·с$^{-1}$/2.7%	Decoy-st./в.к.
				45 км/14.5 дБ	304 кбит·с$^{-1}$/3.8%	Decoy-st./ф.к.
				90 км/27 дБ	2.1 кбит·с$^{-1}$/2.3%	DPS/ ф.к.
[10]/2013	США/NQC	Лос-Аламосская лаборатория	3	25 км	н.д.	Decoy-st./ф.к.
				50 км (на катушке)	н.д.	
[25]/2014	Китай/HCW	Хэфэй, Чаоху, Уху/ USTC	9	8 городских линий/ от 0.9 км/1.2 дБ	от 16.2 кбит·с$^{-1}$/н.д.	Decoy-st./ф.к
				до 16.9 км/6.1 дБ	до 1 кбит·с$^{-1}$/н.д.	
				2 межгородские линии/ 69.7 км/14.1 дБ	0.77 кбит·с$^{-1}$/н.д.	
				85 км/18.4 дБ	0.8 кбит·с$^{-1}$/1.16%	
[26]/2017	РФ/проект без названия	Москва/РКЦ	3	15 км/7 дБ	0.1 кбит·с$^{-1}$/н.д.	BB84/ф.к.
				30 км/13 дБ	0.02 кбит·с$^{-1}$/н.д.	

Примечание: ф.к. – фазовое кодирование, п.к. – поляризационное кодирование, в.к. – временное кодирование, д. – детектирование, н.д. – нет данных, г.д. – гомодинное детектирование.

дами спектрального уплотнения (мультиплексирования) каналов WDM. Кроме того, между городами Хэфэй и Уху была развернута сеть КРК (рис.3) с фазовым кодированием кубитов [25], развивающая концепцию смешанного применения доверенных ретрансляторов и оптических переключателей. В этом проекте ключи КРК были использованы также в виртуальной частной сети VPN (Virtual Private Network), т.е. в сетевом наборе дополнительных средств защиты, создаваемых поверх основной сети. При этом магистральная линия длиной 150 км включала в себя три доверенных узла-ретранслятора. Внутригородская сеть г. Хэфэй основного типа с пятью узлами

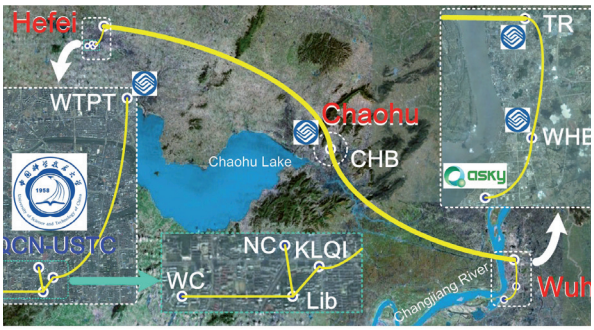


Рис.3. Схема сети КРК в городах Хэфэй–Чаоху–Уху (КНР) [25].

использовала структуру оптических переключателей для связи типа «все-со-всеми», допуская одновременную работу нескольких квантовых линий. Внутригородская сеть г. Уху была выполнена как сеть доступа с временным уплотнением каналов TDM, обеспечивавшим одномоментно работу только одной квантовой линии.

В табл.2 представлены особенности структуры многопользовательских сетей КРК, основные параметры которых даны в табл.1. Следует отметить оригинальную схему основной сетевой магистрали в [23], реализованную как кольцо из трех сетевых узлов на базе управляемых оптических мультиплексоров с грубым разделением каналов по длине волны CWDM (Coarse Wavelength Division Multiplexing) и системой удаленного переключения частотных каналов оптического мультиплексора ROADM (Reconfigurable Optical Add-Drop Multiplexer), подробно описанную в [109]. В [25] в аналогичных целях была реализована схема из трех циркуляторов.

Во всех проектах, указанных в табл.2, был реализован коэффициент разветвления не более 1:4 (один узел соединен с четырьмя), тогда как стандарт GPON (Gigabit-Capable Passive Optical Network) для пассивных ВОЛС обеспечивает значения этого коэффициента до 1:128 [112]. В целом, разветвление сети на базе оптоэлектронных устройств пока значительно отстает от возможностей компьютерного доверенного ретранслятора [8–10], а надежды связаны, прежде всего, с пассивными волоконными разветвителями [109, 110].

Проблемы оптимизации размещения доверенных узлов рассматривались, например, в [19]. Возникновение шумов в волоконных сетях КРК вследствие спонтанного рамановского рассеяния обсуждалось в [20, 109, 110], а возможный подход к решению этой проблемы в сетях доступа был рассмотрен в [107, 108]. В проекте [24] длины воздушных линий составляли половину длины всех использованных ВОЛС, что являлось рекордом.

3. Комбинированные сетевые схемы на базе квантовой оптики и расширенного набора методик компьютерной обработки данных

Среди публикаций по многоузловым сетям особый интерес представляют работы по использованию КРК в сетевых схемах сетецентрических систем (network-centric system) [8–10] и в фотонных сетях (photonic networks) [11, 12], демонстрирующие тенденцию интеграции сетей КРК с мультиагентными моделями искусственного интеллекта [47].

3.1. Сетецентрическая система с архитектурой доверенного третьего лица

Работы, связанные с развитием сетецентрических систем [113, 114], начаты в 1999 г. в рамках проектов DARPA (США) Управления перспективных исследовательских проектов Министерства обороны США. Их цель – создание глобальных одноранговых P2P (Peer-to-Peer) компьютерных сетей военного и гражданского назначения. В таких сетях, в отличие от обычных архитектур «клиент–сервер», все узлы обладают равными коммуникационными возможностями и обеспечивают произвольную маршрутизацию сообщений через любой узел. Это гарантирует самовосстановление и устойчивость работы при потере узлов в критических структурах управления, а также реализует тесное информационное взаимодействие людей и различных видов беспилотных автономных роботов с вычислительными центрами управления, космическими аппаратами и телекоммуникационными сетями. При этом правила взаимодействия агентов и иерархические модели управления коллективом агентов встроены непосредственно в модель поведения каждого агента [47]. Помимо результатов работ [8–10], в концепцию сетецентрических систем хорошо вписываются космические средства КРК [15–17, 34], а также результаты эксперимента [115] по передаче квантовых ключей с борта самолета на наземную станцию.

В [8–10] были представлены результаты проекта Лос-Аламосской Национальной лаборатории США по созданию сетецентрической системы, управляющей критической инфраструктурой энергосети в условиях жесткого централизованного сетевого администрирования работы узлов с ограниченными вычислительными ресурсами. Цель использования КРК заключалась в предотвращении подслушивания или модификации команд управления. В основу этого проекта, защищенного несколькими патентами США, была положена многоуровневая иерархическая архитектура (или топология) «звезда» (рис.4).

В схеме на рис.4 на уровне физических объектов (внизу) подключение большого числа N клиентов к серверу происходит через квантовые линии. На уровне менеджмента КРК (средняя часть рисунка) сервер поддерживает функции доверенного центра управления сертификатами безопасности, контролирующего межузловые сценарии. На уровне приложений (вверху) реализуется так называемое доверенное третье лицо (по сути, программный робот-агент), традиционно именуемое Трент. При этом все компоненты доверенного третьего лица интерпретируются как безусловно безопасные для любого обратившегося к нему клиентского узла (Алиса, Боб, Чарли), а структура распределяемых квантовыми протоколами ключей обеспечивает для доверенной сети конфиденциальность, аутентификацию (проверку подлинности) пользователя и невозможность отказа от обязательств.

В схеме КРК в [8–10] использовался протокол BB84 с состояниями-ловушками, где разработчики кодировали кубиты состояниями поляризации, считая фазовое кодирование слишком требовательным к стабильности интерферометрических схем, громоздким и дорогим. Это, однако, потребовало серьезной борьбы с эффектом двулучепреломления в волокне и создания системы автоподстройки поляризации. Передающий интегрированный модуль передачи квантового ключа включал в себя лазер

Табл.2. Особенности структуры полевых сетей КРК и решаемые практические задачи.

Источник/ год	Способ коммуникации узлов	Тип сети и разветвлений	Реализованные полезные функции
[18]/2005	Оптический переключатель 2 × 2 с программным управлением	Городская сеть со схемой «звезда» с оптическим переключением четырех узлов	КРК с неполнофункциональными узлами: только прием или передача данных. Квантовая аутентификация встроена в обычную архитектуру IPsec и систему обмена ключами IKE
[19]/2009	Доверенный ретранслятор	Городская ячеистая сеть (mesh type) с компьютерным управлением четырьмя полносвязанными узлами и двумя узлами на концах линий КРК	КРК с полнофункциональными узлами. Телефонная связь с шифрованием ОШБ. Видеоконференция с шифрованием AES между всеми узлами. Перемаршрутизация потока данных
[20]/2009	Оптический переключатель 4 × 4 типа 2D-MEMS Оптический мультиплексор DWDM	Лабораторная сеть с одной полевой секцией ВОЛС и оптической динамической перекоммутацией линий	КРК (функции узлов и способ шифрования не указаны). Поток данных КРК встроен в стандартный трафик ВОЛС
[21]/2010	Доверенный ретранслятор Оптический восьмипортовый мультиплексор CWDM	Сеть с межгородской и городскими линиями. «Звезда» с оптическим переключением четырех полносвязанных узлов и автоматической маршрутизацией	КРК с неполнофункциональными узлами. Телефонная связь с шифрованием ОШБ в реальном времени. Видеоконференция с шифрованием AES
[22]/2010	Программное управление коммутацией Оптический мультиплексор CWDM	Схема «звезда» с комплексным переключением и оптическим разветвлением четырех полносвязанных узлов	КРК. Ввод ключа в стандартную систему шифрования AES
[23]/2011	Оптический мультиплексор CWDM с системой ROADM для удаленной коммутации каналов	Городская сеть с основной магистралью – «кольцом» из трех оптических мультиплексоров CWDM и сетью доступа стандарта GPON	КРК с полнофункциональными узлами (способ шифрования не указан)
[24]/2011	Доверенный ретранслятор Иерархическая сеть агентов, которая управляет: – структурой ключей – аутентификацией – выбором маршрута потока данных	Городская ячеистая сеть (mesh type) с компьютерным переключением в кольце из четырех неполносвязанных узлов и двух узлов на конце отдельных линий. Автономный выбор маршрута передачи данных с перемаршрутизацией потока данных в случае обнаружения прослушки	КРК с полнофункциональными узлами. Переключение протокола ОШБ/AES с учетом объема ключа. Защищенная видеоконференция в реальном времени. Защищенная мобильная телефонная связь.Обнаружение прослушки методом отвода части потока фотонов из волокна с компенсацией общего уровня мощности
[10]/2013	Доверенный ретранслятор Компьютерный сервер реализует доверенное третье лицо в стандарте AES с ключом длиной 256 бит	Схема «звезда» с компьютерным переключением: – экспериментально реализовано 1 : 3 – технически возможно 1:1000 – возможно на базе мощного сервера 1 : 1000	КРК с полнофункциональными узлами. Идентификация, аутентификация, шифрование AES и цифровая подпись. Сетецентрическая система защиты процедур сбора критических данных о работе энергосети
[25]/2014	Доверенный ретранслятор Маршрутизатор – «кольцо» из трех циркуляторов с программным управлением и оптическим переключателем 2 × 2	Основная межгородская линия с доверенными комплексными ретрансляторами и оптическим переключением. Городская сеть доступа (access network) с оптическим разветвителем 1 × 2 и TDM	КРК. Полнофункциональные узлы. Телефонная связь с шифрованием ОШБ в сети общего пользования. Ключи КРК использованы шлюзом (роутером) VPN для симметричного шифрования AES с ключом 256 бит
[26]/2017	Доверенный ретранслятор	Городской канал, соединяющий две линии КРК	КРК. Полнофункциональные узлы. Шифрование ОШБ между двумя банковскими офисами

с распределенной обратной связью и модулятор интенсивности, обеспечивавшие для коротких (менее 1 нс) ослабленных импульсов лазерного излучения с $\lambda = 1550$ нм и со средним числом фотонов менее одного на импульс частоту следования 10 МГц. Для измерения квантовых состояний в схеме применялись ЛФД на основе InGaAs с эффективностью обнаружения 15% и вероятностью темновых отсчетов $\sim 10^{-5}$ во временном интервале 1 нс.

При длительном (2.5 года) тестировании использовалась связь доверенного сервера (узел Трент) только с тремя клиентскими узлами (Алиса, Боб, Чарли), однако оборудование принципиально позволяло подключить до 100 узлов, а в случае специального серверного оборудования число клиентов можно было увеличить до 1000. В доверенном узле Трент использовалось временное мультиплексирование сигналов от передающих модулей клиентских узлов. Обработка полученных оптических сигналов ВОЛС выполнялась с помощью стандартного модуля 1000Base-LX. Система обеспечивала одновременную работу квантовых линий для нескольких пар узлов.

В каждом клиентском узле [8–10] использовался КГСЧ оригинальной конструкции с производительностью более 5 Гбит/с. Случайные ключи служили для шифрования с помощью алгоритмов стандарта AES, а алгоритм цифровой одноразовой подписи базировался на схеме Винтернитца. В неквантовых двунаправленных каналах связи использовались процедуры проверки подлинности (аутентификации) узлов с помощью хеш-функций и методики вычисления контрольной суммы с помощью циклического избыточного кода.

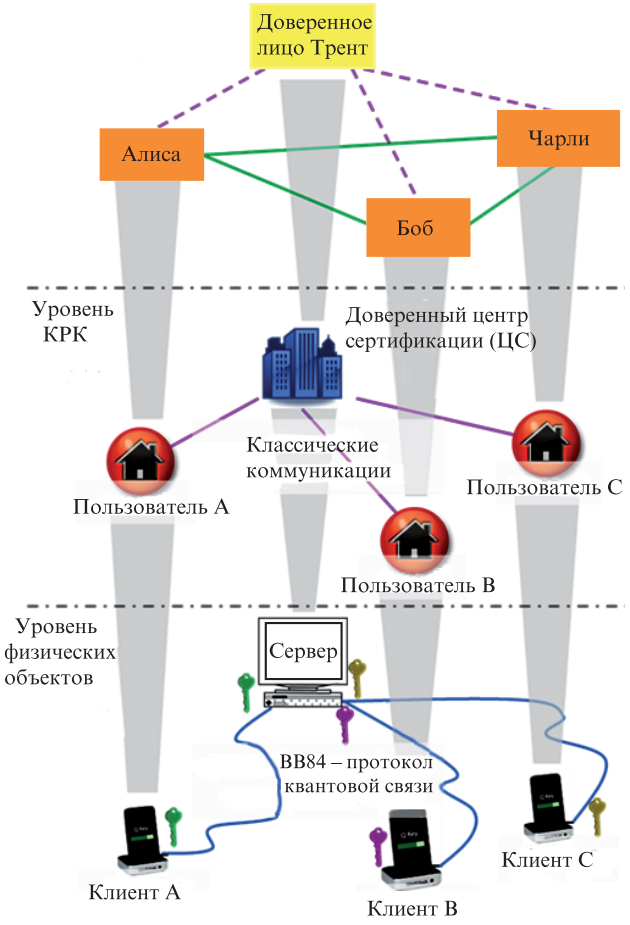


Рис.4. Сетецентрическая архитектура квантовых коммуникаций [10].

Сетецентрическая система КРК [8–10] была успешно протестирована в режиме защищенного сбора параметров работы энергосети, включая процедуры проверки прав доступа абонентов. Уязвимости доверенного сервера в этих работах не обсуждались.

3.2. Фотонная сеть с мультиагентной системой управления ключами КРК

В работе [11], опубликованной в 2011 г. ведущими специалистами из нескольких японских университетов и компаний, была подробно рассмотрена квантовая архитектура, являющаяся разновидностью фотонных сетей [12–14], т.е. чисто оптических телекоммуникационных сетей, ориентированных на массовое обслуживание облачных вычислений или сети цифрового кино. Характерно, что разработчики архитектуры [11] предусмотрели в ней иерархическую структуру аппаратных агентов мультиагентной системы искусственного интеллекта, управляющую квантовыми ключами и обычными криптографическими средствами, а также осуществляющую маршрутизацию потока данных с помощью оптических мультиплексоров и переключателей. Это позволило сократить число доверенных ретрансляторов. Для удешевления в [11] была предусмотрена одна и та же ВОЛС для квантовых и неквантовых каналов КРК.

Как показано на рис.5, архитектура сети [11] имеет пять уровней обмена данными, где схема КРК используется для связи агентов, управляющих распределением ключей. В отличие от используемой в [8–10], управляющая структура аппаратных агентов в [11] является иерархической и имеет единый центр управления ключами (ЦУК). Выделенная подсеть аппаратных агентов контролирует работу оптических перекрестных переключателей

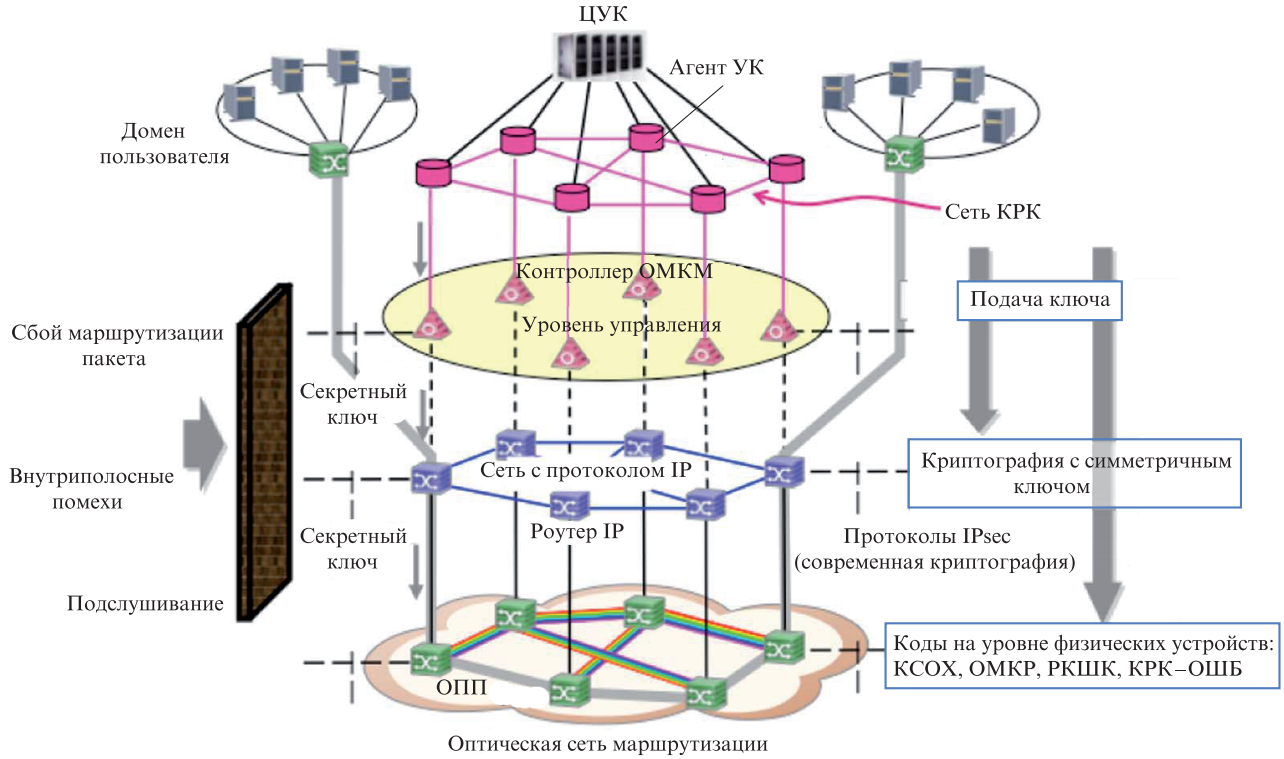


Рис.5. Концептуальная модель квантовой фотонной сети с иерархической мультиагентной системой управления криптографическими средствами [11].

(ОПП), использующих спектральное уплотнение каналов WDM на уровне физических устройств и оптических коммутационных каналов (на рисунке внизу). При этом компьютеры домена пользователей взаимодействуют с IP-маршрутизаторами на уровне обычных сетевых протоколов IP и традиционного шифрования с симметричным ключом. На уровне управления протоколами и сетевыми средствами используется так называемая обобщенная многопротокольная коммутация по меткам (ОМКМ) (GMPLS – Generalized MultiProtocol Label Switching). Именно необходимость обслуживания представленной выше многоуровневой архитектуры в автоматическом режиме без доступа персонала к обрабатываемым структурам данных представляется основным стимулом для внедрения в схемы КРК мультиагентных моделей [8–10, 11, 12], изначально созданных для имитации интеллектуальных функций человека в схемах управления [47]. Кроме того, такие модели необходимы для решения нескольких важных задач классической криптографии, невозможность решения которых средствами квантовой криптографии в настоящее время теоретически обоснована.

Эти задачи, кратко отмеченные в [6, 31], подробно обсуждались в 2016 г. в обзоре [70]. К их числу относятся: невозможность отказа от обязательств (bit commitment), выполнение защищенных двусторонних вычислений (secure two-party computation), доказательство достоверности с нулевым разглашением информации (zero-knowledge proof), реализация функций случайного предсказателя (random oracle), а также позиционно-зависимая криптография (position based cryptography). Для решения всех этих проблем требуется имитировать поведение человека, что оказалось удобнее делать с помощью мультиагентных систем искусственного интеллекта [47].

Помимо совместного применения схем КРК и метода ОШБ (показаны на рис.5 как КРК–ОШБ (QKD–OTP), авторы [11] предложили использовать в фотонных сетях несколько более простых и дешевых методик. Это, например, вариант блочного шифрования в оптической схеме уплотнения каналов с множественным доступом и кодовым разделением каналов (ОМКР) (OCDM – Optical Code Division Multiplexing) [116, 117], а также способ защищенного кодирования рандомизированным квантовым шумом (РКШК) (QNRC – Quantum Noize Randomized Cipher), основанный на протоколе Y-00 [48–51]. Кроме того, в [11] было указано на целесообразность применения в ряде задач схемы защищенного кодирования сигналом «оптического хаоса» (КСОХ) (SCOC – Secure Communications using Optical Chaos) [118], возникающего в излучении ультра-длинного волоконного лазера [119].

Тем самым в [8–12] был продемонстрирован курс на создание для ВОЛС целого набора криптографических средств с различными уровнями цен и криптостойкости. При всем этом мультиагентная система [47] в вышеуказанных работах является гибким средством компьютерного моделирования интеллектуальных функций человека, позволяющим управлять сложным набором квантовых и традиционных криптографических средств.

3.3. Криптографическое кодирование квантовыми шумами передающего лазера

Квантовый протокол Y-00 (обозначаемый также как Yu00 и αη), разработан в 2000 г. в США в рамках проекта DARPA, затем представлен в [48, 49, 120] и других работах этой группы, а также в ряде статей японских ученых [50, 51, 121–128]. При этом защищенное кодирование данных осуществляется с помощью компоненты квантового шума передающего лазера и специальных процедур рандомизации для двух секретных ключей, которые либо заранее заданы отправителю и получателю, либо распределяются отдельной схемой КРК. Протокол Y-00 предназначен для защиты от считывания данных в массовых телекоммуникационных сетях и, в отличие от протоколов КРК, может быть непосредственно использован для высокопроизводительного поточного шифрования с гигабитными скоростями. В работе 2003 г. [48] уровень криптостойкости системы кодирования обеспечивался на уровне стандарта AES, а затем в [121–128] и последующих работах в рамках теории информации Шеннона была обоснована криптостойкость Y-00 к целому ряду классических и квантовых атак.

Режим защищенной передачи для Y-00 [48, 49] осуществлялся путем подключения специальных приемопередающих модулей на входе и выходе уже действующей обычной ВОЛС. В отличие от КРК, Y-00 не требует оптоволокна высокого качества, позволяет использовать волоконные усилители, а также дает возможность применять спектральное уплотнение каналов WDM для увеличения пропускной способности ВОЛС.

В исходных работах [48, 49] протокол Y-00 был реализован по схеме, в которой когерентные квантовые состояния передавались значениями фазы оптического сигнала. Это позволило уже к 2007 г. достичь скорости 2.5 Гбит/с на лабораторной линии передачи данных длиной 210 км [120], а также скорости передачи 622 Мбит/с на полевой линии длиной 850 км. Для массовых сетей на базе ВОЛС в серии работ [50, 51, 121–128] был создан вариант протокола Y-00 с модуляцией интенсивности света. В 2014 г. для этого протокола была продемонстрирована скорость шифрования 100 Гбит/с в ВОЛС длиной 120 км [127].

Общий принцип защищенного многоуровневого, или так называемого M-арного кодирования, используемого в протоколе Y-00 [48], показан на рис.6 для случая кодирования интенсивности света [128]. Используются M различных уровней интенсивности (или фазы для фазового кодирования), задаваемых когерентными состояниями лазерного излучения. Пара таких уровней интенсивности, называемых базисом, служит для кодирования 0 или 1 в передаваемой битовой последовательности. Для каждого передаваемого бита базис выбирается случайным или квазислучайным образом с помощью бегущего ключа, генерируемого из исходно заданного ключа K.

Для наглядности на рис.6 задано $M = 10$ и показаны стрелками пять базисов ($B_1 – B_5$), т.е. всего их $M/2$. При этом в базисах с нечетными номерами значение 0 кодируется большей интенсивностью в паре, а 1 – меньшей. Например, для базиса B_2 значение 1 будет задано уровнем интенсивности 8, а 0 – уровнем интенсивности 3. Соответственно в базисах с четными номерами 0 будет задан меньшей интенсивностью, а 1 – большей. При этом различие между двумя любыми ближайшими уровнями интенсивности настолько мало, что распределения квантовых компонент шума для смежных уровней интенсивности перекрываются и мешают злоумышленнику различать 0 и 1 в передаваемых данных.

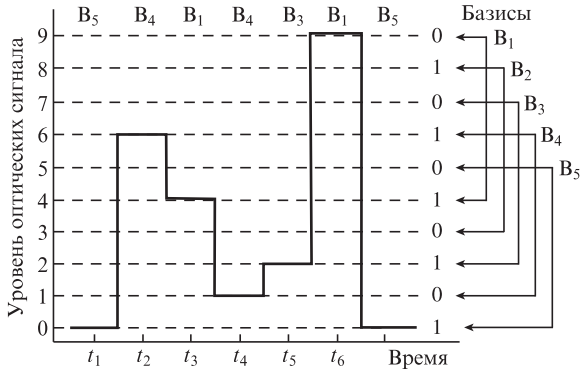


Рис.6. Принцип кодирования протокола Y-00 [128].

Например (рис.7), если в некоторый момент времени с помощью базиса B_4 был передан уровень интенсивности 6 (кодируемый бит содержит 1), то злоумышленник (Ева), измеривший пришедший сигнал, из-за квантовых шумов будет вынужден интерпретировать полученный сигнал как 5, 6 или 7. Но при этом уровни интенсивности 5 и 7 кодируют 0, а уровень 6 – 1. Соответственно, для злоумышленника при передаче 0 и 1 все значения M будут равновероятными, и криптоанализ потребует измерений всего массива передаваемых данных. В то же время с помощью сигналов синхронизации легальный абонент (Боб), знающий исходный ключ K, может расшифровать данные, быстро переключая измерительный базис и выполняя измерения лишь для двух возможных уровней интенсивности с помощью двойного порогового устройства. При этом, конечно, измерение интенсивностей на уровне квантовых шумов требует высокого качества излучателей и однофотонных фотоприемников.

В протоколе Y-00 противодействие криптоанализу данных осуществляется не только путем увеличения параметра $M/2$, используемого в M-арном кодировании, но также повышением равномерности распределения различных блоков 0 и 1 в передаваемом массиве данных [125]. Для этого в [48–51, 120–128] использовали известные приемы работы с блочными шифрами и сдвиговыми регистрами с линейной обратной связью (LFSR – Linear Feedback Shift Register), позволяющими получать из исходного ключа K большой массив квазислучайных значений бегущего ключа. При этом характерные особенности

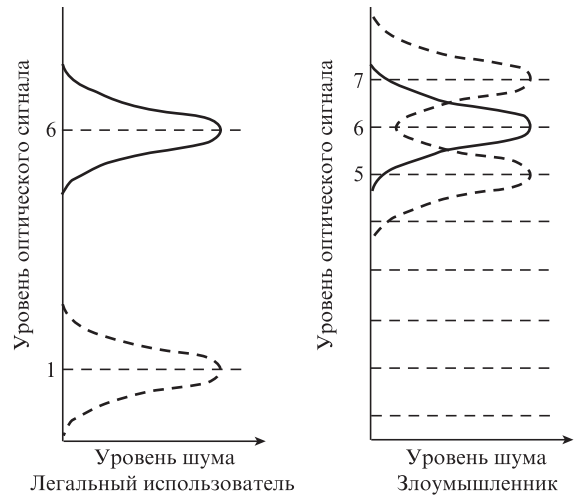


Рис.7. Перекрытие распределений квантового шума для смежных уровней интенсивности оптического сигнала, обозначенных 5–7 [128].

и «слабые» места исходного ключа «размазывают» по большому массиву взаимосвязанных между собой блоков данных длиной M бит, называемых цепочкой блоков (в литературе их нередко называют «блокчейн», что указывает на определенные аналогии с методиками из сферы криптовалют).

Анализ криптостойкости протокола Y-00 сопровождался большим числом дискуссий [129–134]. Авторы [129, 130] провели криптоанализ схемы поточного шифрования, сочетающей протокол Y-00 и метод «одноразового шифроблокнота», для которой ими была рассмотрена атака с использованием известного злоумышленнику текста зашифрованного документа (known plaintext attack). В результате был сделан вывод о том, что реальная криптостойкость Y-00 не может быть выше, чем у традиционного потокового шифрования.

Ответные доводы разработчиков [135–137] сводились к доказательству некорректности использованной в [129–134] методики определения злоумышленником набора битов в бегущем ключе, в которой необоснованно пренебрегали уровнем квантового шума для когерентных состояний. Необходимость учета квантового шума при этом была подтверждена детальными исследованиями группы О.Хироты (Университет Тамагава, Токио, Япония) [138]. Таким образом, в [129] ошибочно игнорировали процедуру усиления секретности ключа. В процессе дискуссии в [135] также удалось показать неэффективность принципиально возможной атаки с использованием гетеродинной схемы измерений, предлагаемой в [129] для взлома Y-00. При этом в целях теоретического обоснования криптостойкости протокола Y-00 авторы [139] на основе вычислений энтропии Шеннона проанализировали нескольких схем индивидуальных квантовых атак (quantum individual attacks). В том числе были рассмотрены варианты атак с использованием только зашифрованного текста, направленные на данные и на ключ, отдельно были проанализированы атаки с измерениями так называемых прямых и непрямых квантовых наблюдаемых атак (direct observable and indirect observable attacks).

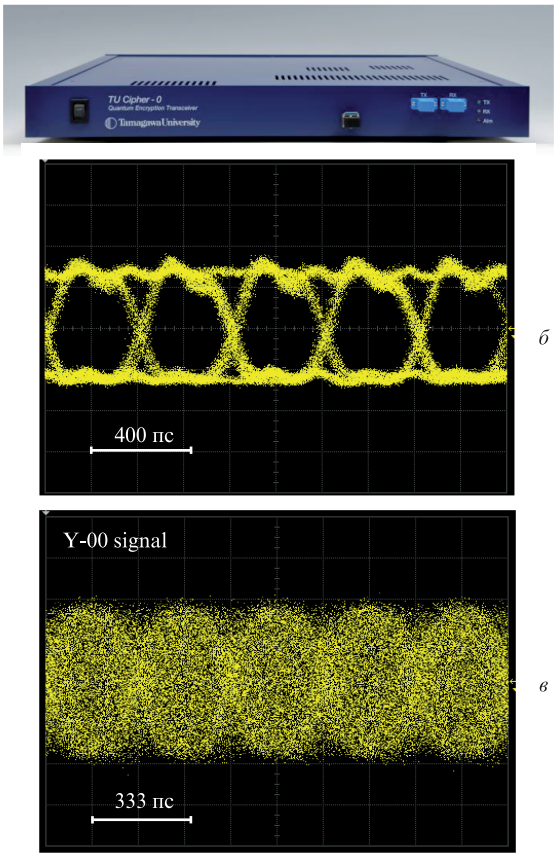
Кроме того, в [139] были рассмотрены атаки с известным или специально подготовленным злоумышленником текстом, а также обычные и модифицированные атаки типа Lo–Ko [131], названные по фамилиям своих разработчиков и предполагающие разделение светоделителем сигнала, отправляемого Алисой, на большое число каналов, а также измерение сигнала в каждом из них отдельным приемником. В частности, авторам [139] удалось показать практическую нереализуемость атак типа Lo–Ko, требующих слишком большого для реального устройства числа каналов. В итоге авторы [139] для целого ряда атак представили доказательство криптостойкости Y-00, обоснованное в рамках теории информации (information–theoretic security). В то же время анализ так называемых непрямых атак на квантовые наблюдаемые атаки привел этих авторов к необходимости увеличения длины исходного ключа K более 100 бит, тогда как в ранних работах авторы Y-00 считали достаточной длину 32 бита.

Помимо этого, подробное рассмотрение более широкого набора квантовых атак для Y-00 было сделано в работе [140], результаты которой подтвердили выводы работы [139]. Кроме того, критические публикации [132–134] в адрес протокола Y-00 заставили внести ряд корректив в экспериментальные схемы. В процессе теоретического моделирования схем Y-00 авторы работы [133]

выяснили, что при наличии затухания и различии амплитуд сигналов, измеряемых Бобом и Евой, более чем в 3 дБ, число регистрируемых Бобом и Евой ошибочных битов заметно перераспределяется в пользу злоумышленника Евы, т.е. возникает дополнительная утечка информации. В итоге разработчикам Y-00 пришлось усложнять экспериментальную схему макета, и в целях дополнительной рандомизации сигнала они добавили специальные быстродействующие модули, вводящие второй псевдослучайный сигнал, независимо получаемый из второго исходного ключа, а длина самих исходных ключей K выросла при этом до 1000 бит. Кроме того, в результате дискуссий [129–134] было скорректировано теоретическое обоснование криптостойкости Y-00.

В результате вышеупомянутых исследований в 2016 г. в [51] было представлено приемопередающее устройство TU-Cipher-0, реализующее протокол Y-00 с гигабайтными скоростями по стандартной волоконно-оптической линии сети Ethernet и использующее 4096 уровней интенсивности. Общий вид устройства показан на рис.8,*а*. Исходный сигнал гигабайтной сети Ethernet и его зашифрованный вариант, полученные с помощью протокола Y-00 на ВОЛС длиной 80 км со стандартным передающим модулем 1000Base-LX, показаны на рис.8,*б*, *в*. В системе используется модуляция интенсивности оптического сигнала ВОЛС с помощью квантового шума лазера отправителя и двух рандомизированных классических ключей, которые можно распределять с помощью схемы КРК.

Для пользователей фотонных сетей с более скромными запросами вместо протокола Y-00 были предложены



а

б

в

Рис.8. Приемопередающее устройство TU-Cipher-0 на базе протокола Y-00 [51]:
а – общий вид; *б* – кодируемый сигнал из гигабайтной сети Ethernet; *в* – выходной сигнал, закодированный по протоколу Y-00.

упоминавшаяся выше схема множественного доступа с кодовым разделением каналов OMKP, а также близкая к ней схема множественного доступа с кодовым разделением абонентов (OCDMA – Optical Code Division Multiple Access) [116, 117, 141–144]. Оба варианта используют принцип спектрального уплотнения каналов WDM, где для упорядочения доступа к общей полосе частот передающей ВОЛС каждый канал кодируется своим набором оптических длин волн (например, двумя значениями λ). Кроме того, в каждом канале за время T передачи одного бита данных осуществляется дополнительный сдвиг короткого оптического импульса по времени, управляемый сдвиговым регистром и M-арным формирователем блочного шифра (аналогично схеме в [51]). Элементная база многоуровневого M-арного кодирования предполагает разработку оптоэлектронных кодирующих устройств, звездообразных разветвителей и маршрутизаторов, мультиплексоров/демультиплексоров на базе матричных волноводных решеток (AWG), волоконных разветвителей, линий задержки, а также оптических переключателей.

Таким образом, разработки на базе протокола Y-00 [48–51, 121–128, 135–140] и оптических схем OCDM/OCDMA [116, 117, 141–144] демонстрируют формирование целого набора более дешевых альтернативных схем, допускающих, в отличие от схем КРК, изменение конфигурации линии, ее ремонт и замену поврежденных секций ВОЛС.

3.4. Возможные схемы атак в квантовых линиях

Атаки на оптическую схему КРК подразделяют [6, 31, 57] на квантовые, выполняемые с измерением квантовых состояний, и классические, реализуемые с помощью обычных измерений. Квантовые атаки подразделяют на индивидуальные и когерентные, в зависимости от измерений одного или нескольких квантовых состояний, а когерентные атаки могут быть коллективными и совместными, в зависимости от воздействия одного или нескольких измерительных устройств на кубит.

Еще в конце 1990-х годов были предложены возможные схемы индивидуальных квантовых атак [78, 87], где каждый кубит измеряется с помощью дополнительных светоделительных элементов и схем перехвата/повторной пересылки кубитов, а также схемы коллективных атак [145], в которых каждое из квантовых состояний измеряется с помощью отдельного зонда.

В обзоре [32] кратко обсуждаются схемы атак на некорректные теоретические модели криптостойкости. Кроме того, разрабатывают методы так называемых слабых измерений [146], которые, в противовес сильным измерениям, не приводят к необратимому коллапсу квантового состояния.

После опубликования экспериментальной работы [99], показавшей возможность создания временных сдвигов квантовых сигналов (time-shift attack) с помощью «врезки» дополнительных волоконных секций, почти нет других публикаций по экспериментальной реализации квантовых атак, что можно объяснить отсутствием практических устройств квантовой памяти. Поэтому в настоящее время наиболее вероятными представляются атаки неквантового типа [6, 31], воздействующие на лазерные источники, модуляторы света или однофотонные фотодетекторы, обзор которых был представлен, например, в [6, 31–33, 57]. Опасность атак неквантового типа заклю-

чается в том, что в них не используется взаимодействие измерительных средств злоумышленника с кубитами и, соответственно, не увеличивается число ошибочных битов, позволяющих обнаружить взлом. Ввиду сложности и дороговизны оборудования для КРК в подавляющем большинстве случаев атаки моделируют теоретически.

В атаках *на источник лазерных сигналов* [32] могут использоваться:

– светоделительные устройства для воздействия на многофотонную компоненту в ослабленном лазерном импульсе [4, 87], что заставило разрабатывать протоколы BB84 с состояниями-ловушками [92];

– высокоэнергетичное разрушение оптических устройств или частичная модификация их параметров (laser damage attack) [147, 148];

– использование в некоторых схемах КРК сразу нескольких лазерных диодов с индивидуальными особенностями спектров или других характеристик [32, 149];

– корреляция импульсов света в излучаемой последовательности [150].

Атаки на модуляторы света, используемые в передающей и принимающей частях схемы КРК, могут быть совершены с использованием лазерных импульсов высокой интенсивности (large pulse attack) [147]. Запуск Евой интенсивного лазерного импульса в передающую линию в сторону Алисы или Боба приведет к отражению компонентами схемы части сигнала, измерение характеристик которого позволит Еве оценить коэффициенты пропускания модуляторов и заданные ими квантовые состояния. Вторая возможность здесь заключается в высокоэнергетичном разрушении оптических компонент (laser damage attack), например аттенюатора на выходе устройства Алисы, снижение коэффициента пропускания которого приведет к усилению эффективности квантовой атаки со светоделительным устройством и неквантовой атаки с использованием лазерных импульсов высокой интенсивности. В [151] представлены более сложные схемы атак троянского типа (Trojan-horse attack) с использованием методов оптической рефлектометрии в частотной области для оценки состояний модуляторов света и других устройств.

Атаки на однофотонные фотоприемники [32, 57] могут, прежде всего, использовать яркие ослепляющие импульсы (tailored bright attack или blinding loophole) [152, 153]. В 2010 г. была продемонстрирована принципиальная уязвимость при такой атаке двух коммерческих установок КРК, разработанных компаниями IDQuantique и MagiQ Technologies [152], а в 2011 г. этот метод взлома был реализован экспериментально на линии КРК длиной в 290 м в Национальном университете Сингапура [153]. В эксперименте с яркими ослепляющими импульсами использовалась уязвимость парных ЛФД, установленных в модуле Боба. В процессе атаки злоумышленник «ослеплял» все ЛФД у Боба с помощью внешнего лазерного диода с непрерывным излучением и круговой поляризацией, а далее по мере необходимости добавлял линейно поляризованные импульсы от четырех других лазерных диодов, искусственно генерируя желаемый сигнал отклика в любом из детекторов Боба. Коэффициент ошибочных квантовых битов QBER при этом оставался на уровне, считавшемся безопасным.

В других видах атак на фотодетекторы могут использоваться:

– широкополосное паразитное световое излучение, испускаемое кремниевым ЛФД при возникновении лавины [154] и попадающее в короткий отрезок (pigtail) волоконного интерферометра;

– уже упомянутая выше схема формирования временных сдвигов [99] с помощью «врезки» дополнительных волоконных секций;

– ввод ложных (faked-state attack) оптических сигналов, порождающих аналогичные регистрируемым при детектировании одиночных фотонов выходные сигналы [155], что осуществимо в схемах атак «человек посередине» (man-in-the middle);

– анализ временных параметров сигнала, измеренного «слишком» точно, с передачей избыточного числа характерных наборов значащих цифр [156];

– зависимость эффективности детектирования фотонов от времени в стробируемых парах фотоприемников, где небольшие различия в характеристиках фотодетекторов и изменение злоумышленником времени прибытия фотона относительно синхроимпульса влияют на отсчет 0 и 1 и облегчают проведение атаки с ложными сигналами [57, 157, 158];

– ввод злоумышленником импульсов, зондирующих схему КРК на значительно отличающихся от рабочих значений длинах волн λ, например $\lambda = 1924$ нм вместо 1536 нм (Trojan horse attack) [159].

Кроме того, злоумышленник может использовать утечки информации по вспомогательным техническим каналам [6, 31, 57]. Модель для оценки возможного объема таких утечек была предложена в [160].

Следует отметить, что приведенные выше схемы атак не исчерпывают всех возможных вариантов, описанных в литературе.

Представленные выше работы помогли сформировать более реалистичный взгляд на уровень проработанности и надежности существующих схем КРК. Например, В.Скарани, соавтор ряда протоколов КРК и работ по анализу уязвимостей, в [32] подчеркнул, что концепция «криптостойкости на основе физических законов» превратилась в значительной мере в рекламный лозунг, часто некорректно трактуемый как «криптостойкость, основанная *только* на законах физики».

Сложность задачи построения целостной модели КРК видна, например, из того, что через 5 лет после успешного использования протокола COW [161] в международном европейском проекте SECOQC [19] появилась статья [93], доказывающая его уязвимость. Кроме того, в ответ на публикацию 2016 г. [162], описывающую новую схему КРК с передачей квантового сигнала на боковой частоте сильного классического оптического сигнала, в статье [163] был обоснован метод ее взлома. Поэтому в недавнем обзоре [57] особое внимание уделялось методам противодействия атакам.

Основные подходы к противодействию атакам заключаются [57] прежде всего в усовершенствовании аппаратной и программной частей схем КРК. Доработки аппаратной схемы включают установку:

– дополнительных оптических изоляторов (вращателей Фарадея) и фильтров, препятствующих распространению введенных Евой оптических сигналов;

– дополнительных контрольных фотодетекторов (watchdog detectors) на входе в устройства Алисы и Боба, отслеживающих уровни входящих сигналов.

Однако для оптических изоляторов открытым остается вопрос о контроле всего диапазона длин волн, способных распространяться в схеме КРК, а для контрольных фотодетекторов может потребоваться варьирование режимов их синхронизации – моментов включения и ширин используемого временного окна.

Усовершенствованные программные средства в схемах КРК необходимы для противодействия атакам, использующим различия спектральных характеристик лазерных источников [57]. В таком случае требуются дополнительные процедуры усиления секретности ключа.

Отдельным направлением является разработка новых схем КРК, в которых особые надежды возлагают на схемы, не зависящие от аппаратной части (DI–QKD, MDI–QKD) [57].

Эксперименты со схемами КРК требуют сложных методик [18–28] и установок стоимостью в десятки тысяч евро, поэтому методы борьбы с атаками квантового и неквантового типа еще не сложились в целостную методику, которая бы позволила с помощью открытых публикаций составить независимое мнение по криптостойкости той или иной схемы КРК.

3.5. Уязвимости компьютерных устройств, обслуживающих сети КРК

В отличие от разработок систем КРК, основанных на академических исследованиях в сфере квантовой оптики, в компьютерных сетях анализ уязвимостей и возможных атак основан на детальном понимании совместной работы конкретного программного кода и аппаратной части, тестируемых с помощью коммерческих программных и аппаратных средств. При этом результаты большинства тестов публикуются в аналитических отчетах специализированных государственных, частных и общественных организаций. В число таких организаций, кроме уже упоминавшегося NIST, входят SANS (США, http://www.sans.org/), CSI (США, http://www.gocsi.com), ASIS (https://www.asisonline.org). Из российских компаний можно выделить АО Лаборатория Касперского (https://www.kaspersky.ru/). Кроме того, собственную аналитику публикует российская компания Infowatch (https://www.infowatch.ru/), а также более мелкие аналитические и информационные агентства, например TAdvisor (http://www.tadviser.ru/). Большое влияние на компьютерное сообщество оказывают такие авторитетные издания и сайты, как http://www.schneier.com/, http://www.wired.co.uk/, http://www.pcworld.com, http://www.cnews.ru/, http://www.cybersecurity.ru/.

Любая современная квантовая линия в многопользовательской сети КРК [8–12, 18–27] не является автономным средством защищенной связи, а представляет собой систему распределения случайных ключей, используемых обычными сетевыми криптографическими средствами для кодирования сообщений. При этом вопрос уязвимости компьютеров, программируемых логических интегральных схем (ПЛИС) и микроконтроллеров, обслуживающих схему КРК и рабочие места абонентов, выходит за рамки лазерной физики и квантовой оптики и практически не рассматривался в литературе по КРК. При описании коммерческих проектов, обсуждаемых, например, на сайте компании Id Quantique [164], специализирующейся на разработке систем КРК, проблема информационной защиты компьютерной компоненты обозначена лишь в общем виде. Между тем, в соответствии с комплексным подходом к обеспечению информационной безопасности вычислительных систем, практикуемым в РФ [71, 72, 165, 166], для всесторонней защиты системы необходимо перекрыть все возможные каналы утечки данных через вычислительные устройства, вспомогательные технические средства и персонал. Используемый для интернета и массовых телекоммуникационных сетей типичный набор средств информационной защиты [72, 165–178] включает в себя:

– антивирусные программные продукты;

– средства борьбы с утечками информации и контроля лояльности персонала;

– антиспамные программные средства;

– средства борьбы с потоками ложных запросов (т. е. DDoS-атаками);

– межсетевые экраны (файерволы) для фильтрации сетевых пакетов с целью защиты от несанкционированного доступа;

– средства шифрования, к которым относится квантовая криптография;

– средства парольного доступа и биометрики для управления идентификацией и доступом;

– специальные системы управления технологическими процессами критически важных объектов;

– системы хранения данных и резервного копирования;

– средства предотвращения утечек данных по вспомогательным техническим каналам (сетям питания, трансформаторам и др.);

– средства защиты от физического взлома устройств.

При этом непосредственное считывание закодированных данных из канала связи, которому противодействует схема КРК, не выделяют в отдельную категорию средств защиты, что можно объяснить широким распространением в массовых сетях алгоритма Диффи–Хеллмана, позволяющего открыто распределять секретные ключи [72]. В литературе не удалось найти данных о случаях массового взлома телекоммуникационных сетей через уязвимости данного инструментария. Соответственно, сети КРК, защищающие от считывания из канала связи, следует заведомо позиционировать как специализированные или нишевые средства, относящиеся к указанной выше категории специальных систем управления технологическими процессами критически важных объектов. В таких системах компьютерная платформа сети КРК должна противостоять всем видам сетевых угроз, но именно здесь имеется много нерешенных проблем.

К наиболее актуальным угрозам для массовых телекоммуникационных сетей относят вирусы, трояны и другие разновидности вредоносных программ, распространяемых по сетям Ethernet и Wi-Fi [167–171]. Как указывалось в [168], необходим поиск принципиально новых подходов к организации систем антивирусной защиты, поскольку, например, в 2012 г. число обращений в службу анализа зараженных файлов лишь только одной компании McAfee (США) в течение месяца превысило 100 млрд. Необходимо создать меры противодействия новым видам вирусов, не позволяющим антивирусным программам собирать и анализировать свой вредоносный код за счет шифрования его уникальными машинно-зависимыми ключами, индивидуальными для каждого зараженного

компьютера [169, 170]. Кроме того, в 2017 г. WannaCry и ряд других вредоносных программ [171] приобрели способность массово шифровать файлы пользователей с требованием выкупа.

Еще одна серьезная проблема защиты информации в компьютерных сетях связана с утечками данных [172–175], возникающими вследствие злонамеренных действий нелояльного персонала. В 2014 г. мировые потери из-за утечек информации составили около $18.5 млрд. Согласно данным [174], в 2016 г. в РФ в результате утечек было скомпрометировано 128 млн. записей конфиденциальных данных, что в 100 раз превышает показатель предыдущего года. В работе [176] были отмечены многочисленные факты целевых (таргетированных) атак, в том числе использующих специфические особенности банковского программного обеспечения.

В работе [173] было подчеркнуто, что критическую уязвимость для компаний представляют их собственные сотрудники и утекающая через них инсайдерская информация. Это заставляет разрабатывать средства аналитики человеческого поведения, многократной проверки биометрической информации на протяжении всего сеанса работы, а также методы борьбы с подделками цифровых фотографий. Разработчики, включая компанию Microsoft, вынуждены внедрять технологии искусственного интеллекта [177, 178], направленные на анализ сетевой активности, контента трафика и контроля лояльности персонала, а также минимизировать участие персонала в процедурах обработки и хранения ключей.

Признанный авторитет в сфере традиционной криптографии Б.Шнайер ранее утверждал [44], что «Математическая криптография даже со всеми своими нынешними изъянами является самым сильным звеном в большинстве цепей общей безопасности…». Однако с традиционными криптографическими методами дискретного логарифмирования, поиска простых множителей и вычислений на эллиптических кривых также имеются проблемы. В частности, в 2012 г. на сайте www.cryptography.ru. в редакционном обзоре отмечалось: «В течение ряда последних лет принципиально новых идей в задаче дискретного логарифмирования и факторизации не появляется…». К тому же стойкость всех схем асимметричной криптографии основана лишь на предположениях о невозможности эффективного вычислительного решения ряда так называемых NP-полных проблем, включая задачи факторизации, разложения на множители больших чисел и логарифмирования в дискретных полях большого размера.

Проведение конкурса NIST по разработке алгоритмов постквантовой криптографии [37, 38], устойчивой и к классическим методам взлома, и к квантовому алгоритму Шора, было обусловлено обнаружением уязвимостей в ранее рекомендованной схеме вычислений на эллиптических кривых [41, 46], что было выявлено именно в процессе анализа алгоритмов для квантового компьютера. С другой стороны, новые методики [37, 38], перспективные как средства усиления неквантовой криптографии, не предоставляют способов решения проблем с вирусами, утечками данных и нелояльным персоналом. При этом метод ОШБ, или совершенного (т.е. невзламываемого) кода Вернама по-прежнему остается наиболее защищенным, а использование в нем истинно случайных последовательностей способно обеспечить абсолютную криптостойкость [74].

4. Направления развития комбинированных схем

4.1. КГСЧ для криптографических и компьютерных систем

Истинно случайный выбор базисов и значений кодирующих параметров в схемах КРК и протокола Y-00 носит принципиально важный характер [2, 4, 6, 31, 57, 59]. Поэтому в рамках работ по лазерным источникам излучения и схемам КРК были предприняты значительные усилия по созданию качественных КГСЧ [52, 53, 179–185].

В обзоре 2016 г. [52] выделены четыре основные схемы создаваемых КГСЧ:

– схема с прохождением фотона в виде суперпозиции горизонтальной и вертикальной поляризаций через асимметричный (поляризационный) светоделительный элемент, пропускающий горизонтальную и отражающий вертикальную составляющую, где значение бита определяется парой однофотонных детекторов;

– схема с прохождением фотона в виде суперпозиции отраженной и прошедшей частей через симметричный (неполяризационный) светоделительный элемент, после чего 0 или 1 генерируется измерением для одного из двух имеющихся путей фотона;

– схема с одним фотодетектором и измерением времени прибытия фотона, где случайные биты определяются измерением интервала времени между двумя последовательно зарегистрированными отсчетами фотонов;

– схема, в которой генерируемое случайное число зависит от пространственного положения фотона, считываемого матрицей однофотонных детекторов.

Более детальную классификацию схем КГСЧ можно найти в [179].

Скорость генерации случайных чисел существенно зависит от выбранной схемы [52]. Например, для схемы КГСЧ с симметричным светоделительным элементом [164, 180], используемой в коммерческих устройствах IDQ Quantis швейцарской компании Id Quantique, скорость генерации случайных битов достигает 4 Мбит/с (в версии платы под шину PCI-E) и ограничивается быстродействием однофотонных неохлаждаемых детекторов [181]. Получаемые последовательности случайных чисел удовлетворяют криптографическим тестам (стандартам) NIST, Diehard, New01, и такие КГСЧ сертифицированы в нескольких странах ЕС. При этом производительность КГСЧ с измеением времени прибытия фотонов составляет более 100 Мбит/с [182]. Она может быть увеличена до ∼1 Гбит/с за счет использования схем, основанных на измерениях флуктуаций вакуумных (нулевых) состояний поля [183] или фазы лазерного излучения [53].

В [53] был представлен модуль КГСЧ с размерами $304 \times 250 \times 78$ мм со встроенными системами температурного контроля и стабилизации фазы, способный в режиме реального времени со скоростью до 3.2 Гбит/с генерировать случайные числа, удовлетворяющие криптотестам NIST. Схема и общий вид устройства КГСЧ показаны на рис.9. Излучение лазерного диода ЛД вводится в несбалансированный компактный интерферометр через циркулятор и симметричный светоделитель СД 50/50, внешние порты которого подсоединены к двум зеркалам Фарадея ЗФ, формирующим интерферометр Майкельсона, не чувствительный к поляризации. Термоэлектрическая система охлаждения (ТСО) выполнена на основе

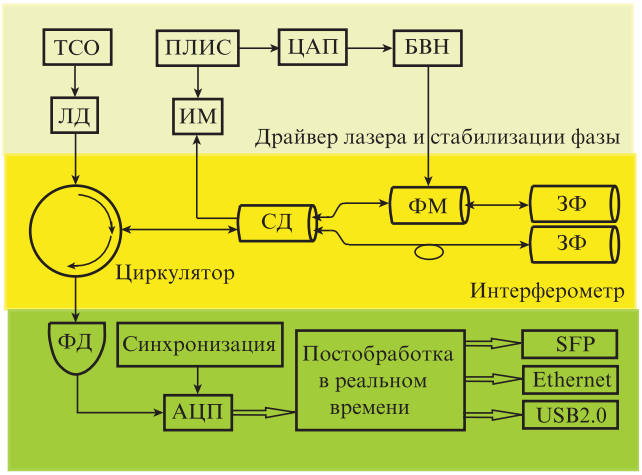


Рис.9. Принципиальная схема устройства КГСЧ с производительностью 3.2 Гбит/с [53].

элемента Пельтье. Фазовращатель ФВ располагается в одном из плеч интерферометра, что обеспечивает различие около 0.8 нс во времени прохождения обоих плеч. К внешнему порту интерферометра через циркулятор подключен фотодетектор ФД (InGaAs, 9.5 ГГц), а другой внешний порт интерферометра контролируется измерителем оптической мощности ИМ на базе другого фотодетектора с АЦП. Далее программируемая логическая интегральная схема ПЛИС работает в режиме пропорционально-интегрально-дифференцирующего регулятора (называемого также PID контроллером), который через ЦАП и блок высокого напряжения БВН управляет фазовым модулятором ФМ, стабилизирующим работу интерферометра.

Случайные данные с фотодетектора ФД поступают через восьмибитный АЦП на ПЛИС, выполняющую в реальном времени сложный алгоритм конвейерной постобработки. Поток случайных чисел со скоростью до 3.2 Гбит/с выводится с помощью стандартного модуля компактных приемопередатчиков для ВОЛС типа SFP (Small Form-factor Pluggable Optical Tranceiver). Кроме того, предусмотрены порт гигабайтного Ethernet (968.7 Мбит/с) и универсальный последовательный порт USB 2.0 (259.5 Мбит/с).

Согласно оценкам [181] оптимизированные величины мощности излучения лазера и скорости выборки данных фазовых флуктуаций позволяют генерировать сырые (необработанные) случайные числа со скоростями до 80 Гбит/с. Однако, как следует из [53, 181], метод их последующей обработки, представленный, например, в [184], является весьма затратным и существенно ограничивает быстродействие КГСЧ. Поэтому в [53] для обработки в реальном времени использовалась быстродействующая ПЛИС Virtex-6 (Xilinx, США) со специально разработанным алгоритмом конвейерной обработки, что в итоге обеспечило скорость генерации до 3.2 Гбит/с.

Таким образом, КГСЧ выделились в самостоятельное направление развития квантовых технологий, базируясь на той же элементной и вычислительной базе, что и схемы КРК. Однако возможности целенаправленного воздействия злоумышленников на КГСЧ обсуждались весьма ограниченно [185].

4.2. «Одноразовый шифроблокнот» на базе КГСЧ и вычислений многозначной логики

Современные разработки КГСЧ дают возможность пользоваться преимуществами метода защищенного многозначно-логического кодирования (МЗЛК) [54, 55], являющегося аналогом метода ОШБ. Этот метод даже на восьмибитной платформе позволяет увеличить размерности пространства случайных одноразовых ключей до 10^{500} и более, а также дает возможность строить защищенные логические модели управления для доверенных устройств мультиагентных и сетецентрических систем. Увеличение размерности пространства ключей при этом направлено на противодействие атакам по методу грубой силы (с прямым перебором ключей) [72], опасным в случае использования облачных сервисов или квантового компьютера.

Метод МЗЛК основан на k-значной алгебре Аллена–Живона [186], где входные и выходные переменные многозначно-логических функций принимают дискретные значения истинности $\{0,1,2,\ldots,k-1\}$ [187]. Произвольная функция $y = F(x_1,\ldots,x_n)$ может быть представлена как в виде таблицы истинности, показанной на рис.10 (вверху), так и в виде эквивалентного логического выражения, составленного из констант $\{1,2,\ldots,k-1\}$, бинарных операторов MINIMUM, MAXIMUM и унарных операторов $X(a,b)$, называемых «Литерал» и задаваемых для входных переменных $x_1,\ldots,x_n$. Многозначно-логическую функцию можно записать в памяти в виде матрицы, которая состоит из пар параметров (a_i, b_j), описывающих все имеющиеся в ее логическом выражении операторы «Литерал». Для реализации метода ОШБ достаточно использовать функции с $n = 30$ входными переменными и $k = 256$ значениями истинности [54]. В минимизированном виде такая функция может быть записана в объеме памяти ~16 кбайт [54, 55]. При заданных значениях k и n логическая функция вычисляется по жестко заданному алгоритму, который удобно использовать по умолчанию. Кроме того, такой алгоритм хорошо «распараллеливается» и позволяет применять ПЛИС.

Традиционные криптографические методики обычно работают с размерностями пространства ключей до $\sim 10^{30}$, однако современная математика принципиально позволяет работать с гораздо большими размерностями [188–190], а инструментарий многозначной логики [55, 191, 192] удобен для реализации высокозащищенных методик ОШБ в глобальных сетевых системах с большим числом активных агентов. Кроме того, метод МЗЛК дает возможность на восьмибитной платформе сгенерировать $\sim 10^{70}$ различных случайных одноразовых ключей без перезаписи памяти кодирующего модуля, что важно для длительной автономной работы [54, 55, 193]. Выигрыш в размерности в методе МЗЛК по сравнению с двоичной логикой обусловлен тем, что для многозначно-логической функции число строк в ее таблице истинности составляет k^n вместо 2^n для булевой логики [187], а число различных логических функций при этом составляет k^{k^n} вместо 2^{2^n}.

Для шифрования сообщений методом МЗЛК абоненты Алиса и Боб, как и в схемах КРК, должны установить в своих кодерах/декодерах отдельные КГСЧ. Кроме того, необходимо заранее конфиденциально сформировать с помощью КГСЧ секретную многозначно-логическую функцию со случайно заданными параметрами [54, 55] и

записать ее в память приемопередающих устройств обоих абонентов. Чтобы построить такую функцию, достаточно сгенерировать два массива случайно заданных k-значных чисел, а далее по определенным правилам сформировать из них матрицу пар параметров (a_i, b_j), полностью описывающую функцию и эквивалентную ей таблицу истинности.

Способ формирования и использования случайных одноразовых ключей в методе МЗЛК, представленный на рис.10 (вверху), подробно описан в [54, 55]. В начале сеанса защищенной связи Алиса с помощью своего КГСЧ формирует одноразовый ключ-подсказку, т. е. последовательность из $n-1$ случайно заданных k-значных чисел. Этот набор данных Алиса вводит в качестве входных переменных $x_2, \ldots, x_n$ в логическое выражение для секретной функции. Далее, последовательно подставляя значения переменной x_1 от 0 до $k-1$, она вычисляет последовательность из k случайных значений выходной переменной $y = f(x_1, \ldots, x_n)$.

Наглядно эта процедура изображена на рис.10, где секретная функция $y = f(x_1, \ldots, x_n)$ изображена в виде таблицы истинности, в которой набор значений $x_2, \ldots, x_n$ выделен штриховым овалом, а вычисленная путем перебора всех возможных x_1 случайная последовательность $f(0,0,\ldots,0), \ldots, f(0,0,\ldots,k-1)$ обозначена овалом в столбце y.

Случайный одноразовый ключ R (рис.10), представляет собой случайную перестановку фиксированной начальной последовательности $R_0 = \{0,1,\ldots,k-1\}$, производимую в ячейках чипа памяти с помощью случайной последовательности $f(0,0,\ldots,0), \ldots, f(0,0,\ldots,k-1)$. Для наглядности на рис.10 показан пример восьмибитной платформы, где Алисой вычислен ключ $R = \{102,5,\ldots,237\}$, с помощью которого она шифрует фрагмент из 256 восьмибитных чисел. Далее Алиса открыто отправляет Бобу использованный ключ-подсказку $x_2, \ldots, x_n$ вместе с закодированным фрагментом. Боб подставляет ключ-подсказку в свою копию секретной функции и вычисляет ключ R, использованный Алисой для кодирования. С его помощью Боб далее находит обратную, т. е. декодирующую последовательность.

Помимо оригинального способа реализации высоких размерностей пространства случайных ключей [54, 55], метод МЗЛК предоставляет новые данные для разработки важных для криптографии схем невозможности отказа от обязательств и позиционно-зависимой криптографии. Исходно авторы пионерской работы по КРК [2], наряду с распределением ключей, считали возможным реализовать и схему невозможности отказа от обязательств, которая необходима, когда оба партнера не вполне доверяют друг другу. Основная идея здесь заключается в возможности предварительно отправить получателю «коробку» с секретной информацией, ключ к которой присылают позднее, гарантировав при этом целостность сохраненной в ней информации. Невозможность решить эту задачу с помощью схем КРК, обсуждавшаяся в обзорах [6, 70], в итоге ограничила функции квантовой криптографии только задачами распределения ключа.

Однако в ряду разработок МЗЛК имеется алгоритм, который, как представляется, можно использовать для решения указанной выше задачи в сетевых доверенных узлах, не обладающих безусловной криптостойкостью, но защищенных на уровне кодов ОШБ с рекордной размерностью пространства ключей. Этот алгоритм был предложен в [191] для управляемого упорядочения/разупорядочения структуры нечетко-логических знаний в схеме дистанционного отключения/включения робототехнических устройств. Поскольку набор нечетко-логических правил «Если…То…» и сопутствующих функций принадлежности, используемый системой управления ро-

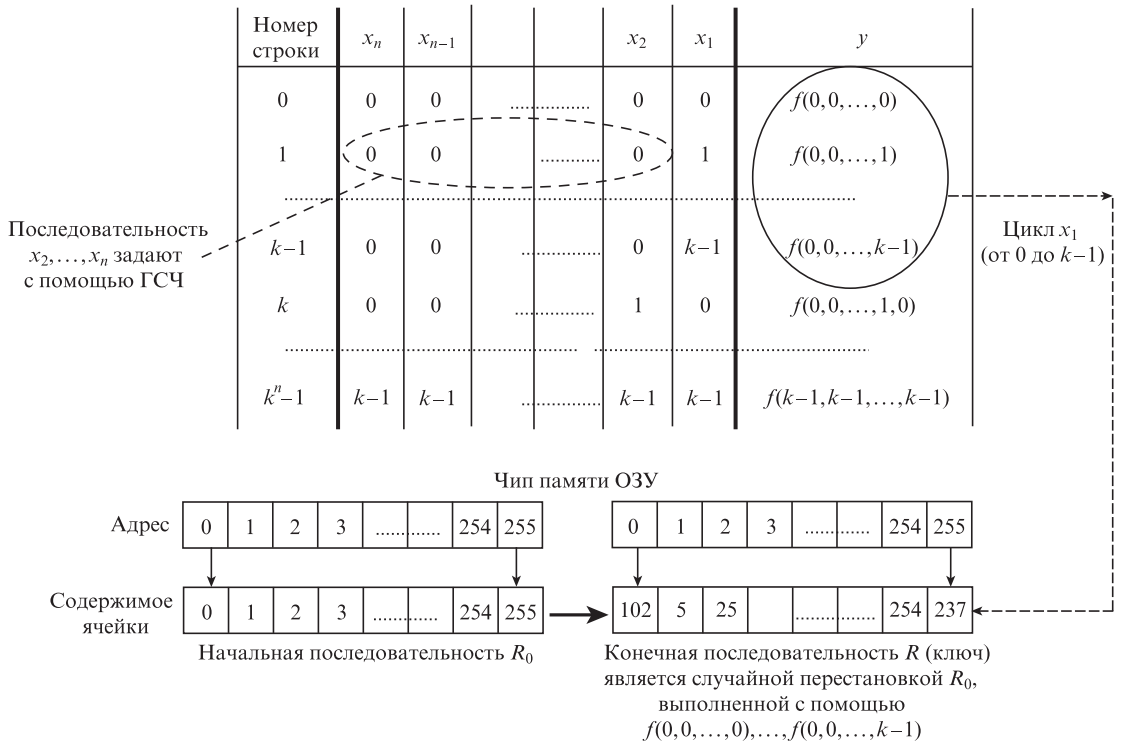


Рис.10. Способ формирования ключей в методе МЗЛК путем вычисления случайной последовательности $f(0,0,\ldots,0), \ldots, f(0,0,\ldots,k-1)$ с помощью случайно выбранного ключа-подсказки $x_2,\ldots,x_n$ и перебора x_1 от 0 до $k-1$ [55].

бота, может представлять собой ценную структуру знаний, то при отключении робота ее целесообразно зашифровать, сделав недоступной для злоумышленников. Такой алгоритм защищенного кодирования на базе МЗЛК можно реализовать в атмосферной лазерной линии связи, соединяющей удаленный цифровой «Ключ» и цифровой «Замок», установленный на роботе. «Замок» регулирует доступ его внутренних подсистем к перекодировочным таблицам, хранящимся в выделенном оперативном запоминающем устройстве (ОЗУ). С помощью нескольких многозначно-логических функций и вспомогательных последовательностей «Ключ» позволяет дистанционно стереть и впоследствии восстановить в выделенном ОЗУ перекодировочные последовательности, управляющие доступом подсистем агента к управляющей структуре знаний.

Чтобы с помощью алгоритма [191] реализовать основную часть схемы невозможности отказа от обязательств [70], достаточно использовать его в устройстве отправителя Алисы и прислать получателю Бобу уже зашифрованную структуру данных (т.е. секретное содержимое «коробки»!), а на этапе ее восстановления прислать ему набор недостающих перекодировочных последовательностей для ее расшифровки. Для полноценной реализации всей схемы невозможности отказа от обязательств необходимо убедить Боба в отсутствии злоупотреблений со стороны Алисы, предоставив ему алгоритм проверки единственности восстанавливаемого сообщения. Разработка такого алгоритма пока не завершена.

Подход к решению другой важной задачи, а именно позиционно-зависимой криптографии, был представлен в работе [192] при обсуждении алгоритма построения многопараметрической карты местности, описываемой с помощью формализма многозначной логики. Если координаты, время и характеристики объектов карты местности описать частью входных переменных таблицы истинности многозначно-логической функции, а другую часть ее входных переменных использовать для ввода пароля, то соответствующее логическое выражение может служить в качестве защищенной цифровой карты высокой информационной емкости. При необходимости такую цифровую карту местности можно дополнительно зашифровать методом МЗЛК, закодировав набор логических констант и параметров операторов «Литерал».

Для реализации интеллектуальных алгоритмов поведения агентов мультиагентных систем и при работе с неточно измеренными данными позиционирования объектов соответствующий аппарат нечеткой логики (набор функций принадлежности и нечетких правил «Если…То...») может быть записан в виде логических выражений алгебры Аллена–Живона [193] в рамках гетерогенной логической модели агента [194]. Тем самым метод МЗЛК позволяет в рамках единого математического формализма описывать для сети агентов их протоколы кодирования по методу ОШБ, правила совместной работы агентов и правила отклика агента на показания цифровых и аналоговых датчиков. При этом метод МЗЛК гарантирует получение точной логической модели для произвольного числа переменных и содержимого таблицы истинности, хотя для быстрых вычислений нужна затратная процедура логической минимизации полученной функции методом консенсуса [186], требующая использования методов многокритериальной оптимизации [195].

4.3. Проблемы, тенденции и задачи развития систем КРК и комбинированных схем

Как было показано выше, современные схемы КРК являются сетевым средством распределения ключей в компьютерной сети, но не самостоятельным видом коммуникационных сетей. Поэтому для решения новых практических задач и создания соответствующих разновидностей сетей, например, сетецентрических систем [8–10] или фотонных сетей [11–13], помимо схем КРК и компьютерных сетей используются новые методы обработки информации, включающие мультиагентные подходы и протоколы кодирования Y-00 и МЗЛК. С учетом этого выделим ряд проблем, сдерживающих развитие квантовой оптики и коммуникационных сетей и требующих первоочередного решения.

1. В области исследований схем КРК важнейшее значение имеет разработка пригодных для практической работы устройств квантовой памяти для ретрансляторов и схем сетевого разветвления линий КРК [6, 8–12, 18–27, 31–33, 35, 69, 196]. Такие устройства позволили бы решить проблемы дальности распределения квантовых ключей по ВОЛС и создания многопользовательских коммуникационных сетей, а также перейти от доверенных ретрансляторов на базе обычных компьютеров к квантовым доверенным узлам. При этом отдельного анализа требуют вопросы уязвимости самих устройств квантовой памяти.

2. Для квантовых линий остается весьма актуальной проблема повышения скорости КРК, максимальная величина которой (более 1 Мбит/с в лабораторных условиях и 304 кбит/с в полевых условиях [24]) слишком мала для поточного шифрования методом ОШБ даже при длине ВОЛС менее 50 км [24, 35, 103, 121, 122]. Современные ВОЛС принципиально способны освоить скорости КРК 100 Гбит/с и более, поэтому необходимы принципиально новые схемы КРК большей производительности.

3. Увеличение длины квантового канала более 80–100 км сопровождается резким снижением скорости КРК до уровня 1–10 кбит/с и менее [18–27, 33, 35, 103, 106]. Этого достаточно лишь для нишевых приложений, примерами которых являются мультиагентные средства управления фотонной сетью [11, 12] и системы защищенной телефонии [19, 21, 24, 25]. Кроме того, хотя использование менее эффективных алгоритмов стандарта AES вместо ОШБ в архитектурах доверенного узла или доверенного третьего лица [8, 11, 19, 21–25] и позволяет обслуживать критическую инфраструктуру управления энергосетью [8–10] и защищенную передачу видеоизображений [19, 21, 24], но при этом уровень защищенности системы в целом, определяемый слабейшими компонентами, снижается до уровня защищенности обычных сетей. Альтернативным решением является либо разработка принципиально новых схем КРК, либо развитие космических систем [15–17, 34,], обеспечивающих в условиях космического вакуума дальности КРК более 1000 км.

4. Проблема эффективного разветвления линии КРК в многопользовательскую сеть также еще не решена [8–12, 18–27, 35] ввиду отсутствия практических устройств квантовой памяти и наличия высоких потерь в оптических схемах разветвления оптоволокна с помощью оптических переключателей, циркуляторов и мультиплексоров. Для КРК реализованы полевые сети с коэффициен-

том разветвления не более 1 : 4 [18, 19, 21, 22, 24], что существенно меньше показателя 1 : 128, предусматриваемого стандартом GPON для пассивных ВОЛС. В то же время на базе чисто компьютерной архитектуры доверенного лица (сервера) в схеме «звезда» обеспечивается коэффициент разветвления до 1 : 1000 [8 – 10].

5. Полный взлом в 2010-11 гг. двух коммерческих макетов КРК [152, 153] существенно усилил внимание к разработке методик защиты от различных типов квантовых и неквантовых атак [32, 33, 147 – 151, 154 – 159, 161, 162], а также показал важность привязки исследований уязвимости к экспериментальным исследованиям реальных ВОЛС и сетей. Однако до сих пор обнаруживаются очередные уязвимости уже известных и новых схем КРК [160, 163]. Способы защиты от возможных квантовых атак исследованы недостаточно. К тому же в литературе нет описания методик, позволяющих читателю независимо от разработчиков и производителей оборудования оценить уязвимости интересующей схемы КРК.

6. Устройства КГСЧ [52, 53, 179 – 185], реализованные на элементной базе схем КРК, достигли гигабитной производительности и пригодны не только для обслуживания протоколов КРК, но и для использования во многих других областях компьютерной техники. Снижение их размеров и веса откроет возможность для более широкого применения, в том числе в стационарных и мобильных устройствах сетецентрических систем. Однако уязвимость самих КГСЧ к атакам квантового и неквантового типа остается малоизученной.

7. В современных многоузловых схемах КРК значительные усилия затрачиваются на создание вспомогательных систем стабилизации температуры, фазы и поляризации света в ВОЛС [8 – 13, 19, 83]. При этом комплект оборудования КРК для одной пары абонентов стоит десятки тысяч долларов и евро. В то же время дополнительное разветвление ВОЛС или ее ремонт путем замены отдельных коротких секций оказывается проблематичным вследствие значительного роста оптических потерь в разъемных или сварных соединениях [83].

8. Важное значение для дальнейшего развития схем КРК имеет совершенствование фотоприемников, а также волоконно-оптических и интегрально-оптических компонентов, обсуждение уровня разработок которых представлено в обзорах [33, 35]. Отдельной проблемой является также совершенствование оптоэлектронной элементной базы фотонных сетей.

9. В литературе практически не удается обнаружить открытые публикации по анализу уязвимостей компьютерной сети, сопрягаемой с системой КРК. В то же время в рамках комплексного подхода [71, 72] к решению проблем информационной безопасности компьютерных систем, практикуемого в РФ, квантовые и обычные средства защиты информации должны анализироваться как единое целое. При работе с глобальной сетью наибольшую опасность представляют воздействия вредоносного кода и злонамеренные действия персонала [167 – 178].

Для коммуникационных сетей на базе КРК самым важным направлением остается развитие глобальных телекоммуникационных средств [7, 24, 33, 35, 63 – 70, 143, 144], требующих гигабитных скоростей распределения ключей, что на несколько порядков превышает возможности известных разработок КРК. В настоящее время наиболее защищенный метод ОШБ удается применить лишь в специализированных нишевых сетевых схемах с ограниченным потоком особо ценных данных [19, 21, 24, 25], вероятность попыток прямого считывания которых из ВОЛС велика. Для массовых телекоммуникационных сетей, где непосредственное прослушивание канала злоумышленником менее вероятно, сфера применения метода ОШБ существенно ограничена стоимостью конкретных разработок. Это делает потенциально востребованным широкий спектр комбинированных схем с различным уровнем криптостойкости.

Для комбинированных схем на базе КРК, создаваемых на основе фотонных сетей [11 – 13], перспективным направление является использование мультиагентных иерархических схем. Это обусловлено, с одной стороны, существенными оптическими потерями в устройствах разветвителей и мультиплексоров, вынуждающими использовать сложные схемы коммутации оптических каналов, а с другой стороны, необходимостью многоуровневого интеллектуального управления сложной структурой коммутирующих устройств и протоколов. Второй важный аспект применения мультиагентных схем для управления фотонными сетями заключается в возможности реализовать автономные доверенные узлы и минимизировать доступ обслуживающего персонала к структурам ключей и передаваемых данных. Кроме того, с помощью модели агента можно облегчить разработку интеллектуальных средств обнаружения и классификации несанкционированных действий нелояльных сотрудников [172 – 177].

В проекте сетецентрической системы защищенного управления энергосетью [8 – 10] комбинированная схема с доверенным третьим лицом была вынужденно сопряжена с традиционным шифрованием стандарта AES, несмотря на необходимость максимальной степени защиты для всех сетевых компонентов. Соответственно, для сетецентрических систем управления критической инфраструктурой актуальна задача использования схем ОШБ на всех уровнях архитектуры обработки протоколов. Именно для этого вида коммуникационных сетей наиболее востребованы комбинированные схемы, сочетающие работу КРК с методом МЗЛК для реализации доверенных узлов. Такие системы нуждаются также в разработке автономных интеллектуальных устройств для верификации абонентов и сенсорного контроля физической целостности узлов сети КРК.

Другая важная задача развития глобальных сетецентрических систем связана с необходимостью защиты каналов связи стационарных и мобильных агентов [113, 114]. Развитие космических сетецентрических систем может оказаться приоритетным направлением при создании основных (магистральных) линий связи для сети стационарных объектов управления логистикой и беспилотным транспортом. Однако для наземных мобильных роботов сетецентрической системы, работающих в условиях вибраций и пыли, подключение к космическим магистральным линиям КРК [15 – 17, 34] является проблематичным. В этом случае возможна и целесообразна реализация метода ОШБ на базе КГСЧ, МЗЛК и неквантовых атмосферных линий связи. Как можно предполагать, для специализированных видов сетей могут оказаться технически и экономически целесообразными дублирующие режимы передачи данных интенсивными лазерными импульсами по протоколу МЗЛК, запускаемые в случае возникновения внешних искусственных помех или передачи на большие расстояния.

Актуальным представляется создание комбинированных сетевых систем для реализации схем позиционно-зависимой криптографии и невозможности отказа от обязательств, которые не удается решить в схемах КРК [70]. Здесь может быть применен метод многозначно-логической многопараметрической зашифрованной карты [188], описывающей в виде логического выражения взаимосвязь пространственных координат и времени с характеристиками объектов, отображаемых на карте местности. Для удаленного доступа к данным такой секретной карты, хранящейся в доверенном узле или в агенте, часть кода доступа можно вводить по квантовой линии с ограниченной производительностью, а другую часть кода передавать методом МЗЛК по более скоростной неквантовой линии.

Схемы МЗЛК также могут быть использованы для объединения в единую сеть линий КРК, имеющих низкие оптические потери, с фрагментами ВОЛС, подключаемыми оптическими разъемами, мультиплексорами или сваркой ВОЛС, для которых характерны более высокие уровни оптических потерь.

5. Заключение

1. За последние годы в результате теоретических и экспериментальных исследований схем квантовой оптики, а также развития лазерной и волоконной техники и однофотонных фотодетекторов был успешно реализован целый ряд протоколов передачи кубитов на значительные расстояния. Исследованы различные схемы КРК, реализуемые на базе ВОЛС с низким (0.2 дБ/км) и ультранизким (0.16 дБ/км) уровнем оптических потерь. Продемонстрирована работа линий КРК в составе сетевых ВОЛС с криптографическим кодированием методами ОШБ и AES, включая линии передачи телефонных сигналов и изображений. Выполнен ряд проектов многопользовательских сетей КРК.

2. Внедрение схем КРК в массовые телекоммуникационные сетевые ВОЛС сдерживается в настоящее время следующими факторами:

– фактически достигнутая скорость распределения ключа в ВОЛС длиной до 50 км составляет ~1 Мбит/с, тогда как гигабитные телекоммуникационные ВОЛС с поточным шифрованием наиболее защищенным методом «одноразового шифроблокнота» требуют скоростей КРК в ~1 Гбит/с и выше;

– длина ВОЛС более 80–100 км приводит к резкому снижению скорости КРК до уровня ~1 кбит/с, что ограничивает практические применения;

– отсутствует квантовая память, практически пригодная для ретрансляторов и доверенных узлов, что препятствует увеличению длины линий КРК и их разветвлению в сеть, а также вынуждает интегрировать их с традиционными доверенными серверами;

– высокие требования схем КРК к уровню оптических потерь в ВОЛС резко ограничивают число сварных и разъемных соединений оптоволокна.

3. Наличие указанных выше нерешенных проблем является причиной разработки комбинированных сетевых схем, сочетающих усложненные компьютерные методы обработки со схемами КРК. Такие сетевые схемы демонстрируют вынужденное сближение квантовой оптики и компьютерных методов для решения все усложняющихся задач информационной безопасности. В последние годы разработаны такие варианты комбинированных схем, как сетецентрические системы управления энергосетями и фотонные сети для массовых телекоммуникационных и облачных сервисов, где для эффективного управления сложной структурой криптографических средств используют программные и аппаратные мультиагентные системы, имитирующие интеллектуальные функции человека.

4. Для массовых телекоммуникационных приложений в США и Японии создано несколько вариантов комбинированных квантово-классических сетевых устройств защищенного кодирования на базе протокола Y-00, в которых используется двойное криптографическое кодирование, сочетающее средства шифрования AES с модуляцией оптического сигнала по интенсивности или фазе квантовым шумом лазера передающего устройства. При этом для протокола Y-00 с модуляцией по интенсивности осуществлено шифрование стандарта AES со скоростями до 2.5 Гбит/с при длине ВОЛС до 120 км без волоконного усилителя. В отличие от схем КРК, эти разработки позволяют использовать стандартные волоконные усилители и мультиплексоры.

5. На платформе современных аппаратных разработок КГСЧ могут быть построены комбинированные сетевые схемы многозначно-логического защищенного кодирования, позволяющие реализовать аналог метода ОШБ с пространством случайных одноразовых ключей высокой размерности (более 10^{500}) на восьмибитной платформе. Такие схемы основаны на вычислениях дискретных функций k-значной алгебры Аллена–Живона и позволяют обеспечить длительную работу передающих устройств автономных агентов без перезаписи секретных функций. Методика МЗЛК хорошо совместима с мультиагентными подходами искусственного интеллекта, а также с моделью многопараметрической цифровой карты местности. Благодаря этому появляются новые возможности для решения задачи позиционно-зависимой криптографии и реализации схемы невозможности отказа от обязательств, важных с точки зрения построения доверенных узлов.

В целом, острота и разнообразие проблем информационной безопасности в области глобальных коммуникационных сетей требуют значительного расширения объема разработок и совершенствования как чисто квантовых криптографических устройств, так и комбинированных оптоэлектронных систем, для которых достижения квантовых технологий дополняются современными компьютерными разработками и методами искусственного интеллекта.

Работа выполнена при финансовой поддержке Минобрнауки РФ, уникальный идентификатор RFMEFI61615X0060.

6. Литература

1. Wiesner S. *SIGACT News*, **15**, 78 (1983).
2. Bennett C.H., Brassard G., in *Proc. IEEE Intern. Conf. Comput., Syst. Signal Proces*. (New York: IEEE, 1984, p. 175).
3. Bennett C.H., Brassard G. *IBM Tech. Discl. Bull.*, **28**, 3153 (1985).
4. Bennett C.H., Bessette F., Salvail L., Brassard G., Smolin J. *J. Cryptology*, **5**, 3 (1992).
5. Brassard G.A. https://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html.
6. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74** (1), 145 (2002).
7. Agrell E. et al. *J. Opt*., **18**, 063002 (2016).

8. Hughes R.J., Nordholt J.E., et al., in *Proc. 3rd Int. Conf. Quantum Cryptography* (Canada, Waterloo, 2013, LA-UR-13-22718); http://2013.qcrypt.net/program/#invited.
9. Hughes R.J., Nordholt J.E., et al., in *Proc. Frontiers in Optics 2013* (USA, Orlando, Florida, 2013, FW2C, FW2C.1); https://www.osapublishing.org/conference.cfm?meetingid=56&yr= 2013#FW2C or https://doi.org/10.1364/FIO.2013.FW2C.1.
10. Hughes R.J., Nordholt J.E., et al. http://lanl.arxiv.org/ftp/arxiv/papers/1305/1305.0305.pdf.
11. Kitayama K-I., Sasaki M., et al. *J. Lightwave Technol*., **29** (21), 3209 (2011); DOI: 10.1109/JLT.2011.2166248; https://www.researchgate.net/publication/224255782.
12. Kitayama K.-I., Fukui M., et al. https://ieeexplore.ieee.org/document/6825163/.
13. Hughes R.J. et al. *Proc. SPIE*, **5893**, 589301 (2005).
14. Маккавеев В. *Компоненты и технологии*, **55**,142 (2006); http://www.kit-e.ru/articles/telecommunication/2006_2_142.php.
15. Yin J., Cao Y., et al. *Science*, **356** (6343), 1140 (2017); DOI: 10.1126/science.aan3211; http://science.sciencemag.org/content/356/6343/1140/tab-pdf.
16. Liao S.-K. et al. *Nature*, **549**, 43 (2017); DOI: 10.1038/nature23655; http://www.nature.com/articles/nature23655.
17. Ren J.-G. et al. *Nature*, **549**, 70 (2017); DOI: 10.1038/nature23675, http://www.nature.com/articles/nature23675.
18. Elliott C. et al. *Proc. SPIE*, **5815**, 138 (2005); https://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf.
19. Peev M. et al. *New J. Phys*., **11**, 075001(2009).
20. Chapuran T.E. et al. *New J. Phys*., **11**, 105001 (2009).
21. Chen T.-Y. et al. *Opt. Express*, **18** (26), 27217 (2010); DOI: https://doi.org/10.1364/OE.18.027217; https://www.osapublishing.org/oe/abstract.cfm?uri=oe-18-26-27217.
22. Mirza A., Petruccione F. *J. Opt. Soc. Am. B*, **27** (6), A185 (2010).
23. Lancho D. et al. *First Int. Conf. Quantum Comm*. (Italy. Naples, 2009, p. 142); DOI: 10.1007/978-3-642-11731-2_18; https://arxiv.org/abs/1006.1858v2.
24. Sasaki M. et al. *Opt. Express*, **19** (11), 10387 (2011).
25. Wang S. et al. *Opt. Express*, **22** (18), 021739 (2014).
26. Киктенко Е.О., Пожар Н.О., Дуплинский А.В. и др. *Квантовая электроника*, **47** (9) 798 (2017) [*Quantum Electron*., **47** (9), 798 (2017)]; DOI: 101070/QEL16469.
27. Wang S., Chen W., et al. *Opt. Lett*., **35** (14), 2454 (2010).
28. Kiktenko E.O. et al. *J. Phys.: Conf. Ser*., **741**, 012081 (2016).
29. Williams C.J. https://math.nist.gov/mcsd/Seminars/2004/2004-03-23-williams-presentation.pdf.
30. Graham-Rowe D. https://www.technologyreview.com/s/415073/quantum-cryptography-for-the-masses/.
31. Scarani V., Bechmann-Pasquinucci H., et al. *Rev. Mod. Phys*., **81**, 1301 (2009); https://arxiv.org/abs/0802.4155v3.
32. Scarani V., Kurtsiefer C. *Theor. Comp. Sci*., **560**, 27 (2014); https://doi.org/10.1016/j.tcs.2014.09.018.
33. Lo H.-K., Curty M., Tamaki K. *Nature Photon*., **8**, 595 (2014).
34. Bedington R., Arrazola J.M., Ling A. *npj Quant. Informat*., **3**, 30 (2017); DOI: 10.1038/s41534-017-0031-5; https://www.nature.com/articles/s41534-017-0031-5.
35. Diamanti E., Lo H.-K., Qi B., Yuan Z. *npj Quant. Informat*., **2**, 16025 (2016).
36. https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution.
37. https://csrc.nist.gov/projects/post-quantum-cryptography.
38. Chen L. et al. DOI: 10.6028/NIST.IR.8105; https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.
39. https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.
40. Länger T., Lenhart G. *New. J. Phys*., **11** (5), 055051 (2009).
41. http://www.nist.gov.
42. Black P.E., Kuhn D.R., Williams C.J. *Adv. Comput*., **56**, 189 (2002).
43. Румянцев К.Е. и др. *Электротехнические и информационные комплексы и системы*, **7** (1), 58 (2011).
44. Schneier B. http://www.schneier.com/crypto-gram-0312.html#6.
45. Берд К. http://old.computerra.ru/xterra/206486/.
46. Берд К. https://3dnews.ru/940050.
47. Рассел С., Норвиг П. *Искусственный интеллект. Современный подход* (М.: Изд. дом Вильямс, 2006).
48. Barbosa G.A., Corndorf E., Kumar P., Yuen H.P. *Phys. Rev. Lett*., **90** (22), 227901 (2003).
49. Corndorf E., Barbosa G., Liang C., Yuen H.P., Kumar P. *Opt. Lett*., **28** (21), 2040 (2003).
50. Hirota O., Sohma M., Fuse M., Kato K. *Phys. Rev. A*, **72**, 022335 (2005).
51. Futami F. et al. *Proc. SPIE*, **9980**, 99800O (2016); DOI: https://doi.org/10.1117/12.2237852; https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9980/99800O/A-novel-ransceiver-of-the-Y-00-quantum-stream-cipher/10.1117/12.2237852.full
52. Ma X. et al. *npj Quant. Informat*., **2**, 16021 (2016).
53. Zhang X-G., Nie Y-Q., et al. *Rev. Sci. Instrum*., **87**, 076102 (2016).
54. Antipov A.L., Bykovsky A.Yu., et al. *J. Rus. Laser Research*, **27** (5), 492 (2006).
55. Bykovsky A.Yu., Egorov A.A., Rager B.Yu. *Pacific Sci. Rev*., **3**, 140 (2011).
56. Alleaume R., Branciard C., et al. *Theor. Comp. Sci*., **560**, 62 (2014); https://doi.org/10.1016/j.tcs.2014.09.018.
57. Jain N., Stiller B., et al. *Contemp. Phys*., **57** (3), 366 (2016); https://doi.org/10.1080/00107514.2016.1148333
58. Килин С.Я. *УФН*, **169** (5), 507 (1999).
59. Молотков С. *УФН*, **176** (7), 777 (2006).
60. Lo H.-K., Zhao Y. *Encyclop. Comp. Syst. Sci*., **8**, 7265 (2009); https://arxiv.org/abs/0803.2507v4.
61. Корольков А.С. *Information Security/Информационная безопасность*, **6**, 42 (2013); http://www.itsec.ru/articles2rypto/o sovremennom-etape-razvitiya-prikladnoy-kvantovoy-kriptografii/.
62. Gupta N.L., Mehrotra D.R., Saxena A. *INFOCOMP* [S.l.], **8** (1), 65 (2009); http://www.dcc.ufla.br/infocomp/index.php/INFOCOMP/article/view/252
63. Кулик С.П. *Фотоника*, **4**, 28 (2010).
64. Singh H., Gupta D.L., Singh A.K. *IOSR J. Comp. Eng.*, **16** (2), XI, 01 (2014).
65. Iqbal A, Aslam M.J., Nayab H.S. https://www.researchgate.net/publication/298734157.
66. Kute S., Desai C.G. *Indian J. Sci. Technol*., **10** (3) (2017); DOI:1 0.17485/ijst/2017/v10i3/110635.
67. Кулик С.П. *Фотоника*, **2**, 36 (2010).
68. Кулик С.П. *Фотоника*, **3**, 56 (2010).
69. Tokura Y. *NTT Techn. Rev*., **9** (9), 1 (2011).
70. Broadbent A., Schaffner C. *Designs, Codes Cryptogr*., **78** (1), 351 (2016).
71. Герасименко В.А., Малюк А.А. *Основы защиты информации* (М.: ООО Инкомбук,1997).
72. Рябко Б.Я., Фионов А.Н. *Криптографические методы защиты информации* (М.:, Горячая линия-Телеком, 2005).
73. Маккавеев А.П., Молотков С.Н., Помозов Д.И., Тимофеев А.В. *ЖЭТФ*, **128** (2), 263 (2005).
74. Брауде–Золотарев Ю. *Information Security/Информационная безопасность*, **4**, 56 (2014).
75. Wooters W.K., Zurek W.H. *Nature*, **299**, 802 (1982).
76. Zbinden H., Bechmann-Pasquinucci H., et al. *Appl. Phys. B*, **67** (6), 743 (1998).
77. Eraerds P., Walenta N., et al. *New J. Phys*., **12**, 063027 (2010).
78. Lütkenhaus N. *Phys. Rev. A*, **59**, 3301 (1999); DOI: https://doi.org/10.1103/PhysRevA.59.3301; https://journals.aps.org/pra/abstract/10.1103/PhysRevA.59.3301.
79. Zhao F., Li J.-L. *Proc. SPIE*, **7846**, 78460J-1 (2010); DOI: 10.1117/12.866065.
80. Muga N.J., Fereira M.F.-S., Pinto A.N. *J. Lightwave Technol*., **29** (3), 355 (2011).
81. Gobby C., Yuan Z.L., Shields A.J. *Appl. Phys. Lett*., **84**, 3762 (2004).
82. Bennet C.H., Brassard G., Robert J.-M. *SIAM J. Comput*., **17** (2), 210 (1988).
83. Jacak M., Melniczuk D., et al. *Opt. Quantum Electron*., **48**, 363 (2016).
84. Inamori H., Lütkenhaus N., Mayers D. *Eur. Phys. J. D*, **41**, 599 (2007).
85. Shor P.W, Preskill J. *Phys. Rev. Lett*., **85** (2), 441 (2000).
86. Lim C.C.-W., Curty M., Walenta M., et al. *Phys. Rev. A*, **89**, 022307 (2014).
87. Lütkenhaus N. *Phys. Rev. A*, **61**, 052304 (2000); DOI: https://doi.org/10.1103/PhysRevA.61.052304; https://journals.aps.org/pra/abstract/10.1103/PhysRevA.61.052304.

88. Brassard G., Lütkenhaus N., Mor T., Sanders B.C. *Phys. Rev. Lett*., **85** (6), 1330 (2000).
89. Renner R., Gisin N., Kraus B. *Phys. Rev. A*, **72**, 012332 (2005).
90. Scarani V., Renner R. *Phys. Rev. Lett*., **100** (20), 200501 (2008).
91. Beaudry N.J., Moroder T., Lutkenhaus N. *Phys. Rev. Lett*., **101** (9), 093601 (2008).
92. Hwang W.Y. *Phys. Rev. Lett*., **91** (5), 057901 (2003).
93. Молотков С.Н. *Письма в ЖЭТФ*, **93** (3), 194 (2011).
94. Inoue K., Waks E., Yamanoto Y. *Phys. Rev. A*, **68** (2), 022317 (2003).
95. Lo H.-K., Curty M., Qi B. *Phys. Rev. Lett*., **108** (13), 130503 (2012).
96. Comandar L.C. et al. *Nature Photon*., **10**, 312 (2016); https://arxiv.org/pdf/1509.08137.pdf.
97. Ekert A.K. *Phys. Rev. Lett*., **67** (6), 661 (1991).
98. Acìn A. et al. *Phys. Rev. Lett*., **98**, 230501 (2007).
99. Zhao Y., Fung C.H., Qi B., et al. *Phys. Rev. A*, **78**, 042333 (2008); DOI: 10.1103/PhysRevA.78.042333.
100. Fossier S., Diamanti E., Debuisschert T., et al. *New J. Phys*., **11**, 045023 (2009).
101. Winzer P.J. *Opt. Photon. News*, **26**, 28 (2015).
102. Huang M.F. et al. *J. Lightwave Technol*., **32** (4), 776 (2014).
103. Dixon A.R., Yuan Z.L., et al. *Opt. Express*, **16**, 18790 (2008).
104. Gottesman D., Lo H.-K., Lütkenhaus N., Preskill J. *Quantum Inf. Comp*., **4** (5), 325 (2004).
105. Yuan Z.L., Dixon A.R., Dynes J.F., et al. *New J. Phys*., **11**, 045019 (2009).
106. Korzh B. et al. *Nat. Photon*., **9**, 163 (2015); https://arxiv.org/pdf/1407.7427.pdf.
107. Fröhlich B. et al. *Nature*, **501** (6), 9 (2013).
108. Fröhlich B. et al. *Sci. Rep*., **5**, 18121 (2015).
109. Peters N.A. et al. *New J. Phys*., **11**, 045012 (2009).
110. Choi I.,Young R.,Townsend P.D. *New J. Phys*., **13**, 063039 (2011).
111. Yuan Z.L., Kardynal B.E., et al. *Appl. Phys. Lett*., **91** (4), 041114 (2007).
112. *Оптика и компоненты сетей PON.Технология GPON*. Справ.-инф. сайт xdw.ru, разд. 28 (2018); http://www.xdw.ru/rubrics/28/.
113. Cebrowski A.K., Garstka J.J. *U.S. Naval Institute Proc. Magazine*., **124/1/1/**, 139 (1998); https://www.usni.org/magazines/proceedings/1998-01.
114. Затуливетер Ю.С. В сб. *Труды конф. «Технические и программные средства систем управления, контроля и измерения»* (М.: ИПУ, 2010, 000492).
115. Nauerth S., Rau M., Fuchs C., et al. *Nat. Photon*., **7**, 382 (2013); DOI: 10.1038/nphoton.2013.46.
116. Heritage J.P. et al. *IEEE J. Sel. Top. Quantum Electron*., **13** (5), 1351 (2007).
117. Prucnal P.R. (Ed.) *Optical Code Division Multiple Access: Fundamentals and Applications* (New York: Taylor&Francis, 2006).
118. Argyris A. et al. *Nature*, **438** (17), 343 (2006).
119. Zadok A., Scheuer J., et al. *Opt. Express*, **16**, 16680 (2008).
120. Fung C.-H.F., Tamaki K., Qi B., Lo H.-K., Ma X. *Quantum Inf. Comput*., **9**, 131 (2009).
121. Hirota E.O. *Tamagawa Univ. Quantum ICT Res. Inst. Bull*., **5** (1), 5 (2015); http://www.tamagawa.jp/en/research/quantum/bulletin/2015.html.
122. Hirota E.O. *Tamagawa Univ. Quantum ICT Res. Inst. Bull.*, 5 (1), 37 (2015); https://arxiv.org/abs/1511.04671v1.
123. Hirota O., Kato K., Sohma M., Usuda T., Harasawa K. *Proc. SPIE*, **5551**, 206 (2004).
124. Hirota O., Kato K., et al. *Proc. SPIE*, **5833**, 186 (2005); DOI: https://doi.org/10.1117/12.620487.
125. Hirota O. *Phys. Rev. A*, **76**, 032307 (2007).
126. Kato K., Hirota O. *Proc. SPIE*, **8163**, 81630A (2011).
127. Futami F., Hirota O. *Tamagawa Univ. Quantum ICT Res. Inst.Bull*., **4** (1), 15 (2014); https://pdfs.semanticscholar.org/677b/d1c3c7e3fdd4b647cb77a80d5dd0168501cf.pdf.
128. Ohhata K., Hirota O., Honda M., Akutsu S., Doi Y., et al. *J. Lightwave Technol*., **28** (18), 2714 (2010).
129. Nishioka T., Hasegawa T., et al. *Phys. Lett. A*, **327** (1), 28 (2004); DOI: https://doi.org/10.1016/j.physleta.2004.04.083; https://arxiv.org/abs/quant-ph/0310168v2.
130. Nishioka T., Hasegawa T., et al. *Phys. Lett. A*, **346** (1-3), 7 (2005).
131. Lo H.K., Ko T.M. *Quantum Inform. Comput.*, **5** (1), 041 (2005); https://arxiv.org/pdf/quant-ph/0309127v3.pdf.
132. Donnet S., Thangaraj A., Bloch M., et al. *Phys. Lett. A*, **356** (6), 406 (2006); https://www.sciencedirect.com/journal/physics-letters-a/vol/356.
133. Ahn C., Birnbaum K. *Phys. Lett. A*, **370** (2), 131 (2007); https://arxiv.org/abs/quant-ph/0612058v2 .
134. Ahn C., Birnbaum K. *Phys. Lett. A*, **372** (47), 7097 (2008).
135. Yuen H.P, Kumar P., Corndorf E, Nair R. *Preprint* at arXiv:quant-ph/ 0407067v2 (2004); https://arxiv.org/pdf/quant-ph/0407067v2.pdf.
136. Yuen H.P., Kumar P., Corndorf E., Nair R. *Phys. Lett. A*, **346** (1-3), 1 (2005); https://arxiv.org/pdf/quant-ph/0312029.pdf.
137. Yuen H.P, Kumar P., Corndorf E., Nair R. *Phys. Lett. A*, **349** (6), 516 (2005); https://www.sciencedirect.com/journal/physics-letters-a/vol/349/issue/6.
138. Hirota O., Kato K., Sohma M., Fuse M. DOI: 10.1117/12.620487; https://arxiv.org/abs/quant-ph/0410006v1.
139. Hirota O., Kato K., Sohma M., Usuda T.S., Harasawa K. *Proc. SPIE*, **5551**, 206 (2004); DOI: 10.1117/12.561778; https://arxiv.org/abs/quant-ph/0407062v1.
140. Yuen H.P., Nair R., Corndorf E., Kanter G.S., Kumar P. *Quantum Inform. Comput*., **6** (7), 561 (2006); https://arxiv.org/pdf/quant-ph/0509091.pdf
141. Huang J.-F., Meng S.-H., LinY.-C., Chen K.-S., Huang A-C. *Proc. Comp. Sci*., **34**, 39 (2014).
142. Kitayama K., Wada N., Sotobayashi H. *J. Lightwave Technol*., **18** (12), 1834 (2000).
143. Menendez R., Agarwal A., et al. *J. Opt. Netw*., **6** (5), 442 (2007).
144. Kodama T., Nakagawa N., et al. *J. Lightwave Technol*., **28** (1), 181 (2010); DOI: 10.1109/JLT.2009.2033357; https://www.researchgate.net/publication/243479663_Secure_25_Gbits_16-ary_OCDM_block-ciphering_with_XOR_using_a_single_multi-port_endecoder.
145. Biham E., Mor T. *Phys. Rev. Lett*., **78**, 2256 (1997).
146. Katz N., Neeley M. *Phys. Rev. Lett*., **101**, 200401 (2008).
147. Vakhitov A., Makarov V., Hjelme D. *J. Mod. Opt*., **48** (13), 2023 (2001).
148. Bugge A.N., Sauge S., Mardhiyah A., et al. *Phys. Rev. Lett*., **112**, 070503 (2014).
149. Kurtsiefer C., Zarda P., Halder M., et al. *Nature*, **419**, 450 (2002).
150. Lo H.-K., Preskill J. *Quantum Inf. Comput*., **7**, 431 (2007).
151. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. *Phys. Rev. A*, **73**, 022320 (2006).
152. Lydersen L., Wiechers C., Wittmann C., Elser D., et al. *Nature Photon*., **4**, 686 (2010).
153. Gerhardt I., Liu Q., Lamas-Linares A., et al. *Nature Commun*., **2**, 349 (2011).
154. Kurtsiefer C., Zarda P., Mayer S., et al. *J. Mod. Opt*., **48**, 2039 (2001); DOI:10.1080/09500340108240905; https://arxiv.org/abs/quant-ph/0104103v1.
155. Makarov V., Hjelme D.R. *J. Mod. Opt*., **52**, 691 (2005).
156. Lamas-Linares A., Kurtsiefer C. *Opt. Express*, **15**, 9388 (2007).
157. Makarov V., Anisimov A., Skaar J. *Phys. Rev. A*, **74**, 022313 (2006).
158. Wiechers C., Lydersen L., Whittmann C., et al. *New J. Phys*., **13**, 013043 (2011).
159. Sajeed S. et al. *Sci. Reports*, **7**, 8403 (2017); https://www.nature.com/articles/s41598-017-08279-1.pdf.
160. Молотков С.Н. *Письма в ЖЭТФ*, **97** (10), 693 (2013).
161. Stucki D. et al. *Appl. Phys. Lett*., **87**, 194108 (2005).
162. Gleim A.V., Egorov V.I., Nazarov Yu.V., et al. *Opt. Express*, **24** (3), 002619 (2016).
163. Klimov A.N., Kulik S.P., Molotkov S.N., Potapova T.A. *Laser Phys. Lett*., **14**, 035201 (2017).
164. Сайт комп. IdQuantique, www.idquantique.com.
165. Бузов Г.А. Калинин С.В. Кондратьев В.А. *Защита от утечки информации по техническим каналам* (М.: Горячая линия-Телеком, 2005).
166. Рудометов Е.А., Рудометов В.Е. *Шпионские страсти. Электронные устройства двойного применения* (М.: АСТ, Полигон, 2000).
167. *Безопасность информационных систем 2017*. Обзор аналит. агентства TAdviser, РФ; http://www.tadviser.ru/index.php/Статья: Обзор:_Безопасность_информационных_систем.
168. Чернышев М. *Information Security/Информационная безопасность*, **4**, 44 (2012); http://www.itsec.ru/articles2/bypub/insec-4-2012.
169. Lemos R. https://www.technologyreview.com/s/428557/the-latest-threat-a-virus-made-just-for-you/.
170. http://www.itsec.ru/newstext.php?news_id=86277.

171. Бахур В. http://safe.cnews.ru/news/line/2017-06-29_novaya_globalnaya_ataka_shifrovalshchika_podrobnosti.
172. https://www.infowatch.ru/analytics/reports/24616.
173. https://www.infowatch.ru/report2017.
174. https://www.securitylab.ru/news/486600.php; https://www.infowatch.ru/analytics/reports/17962.
175. https://www.devicelock.com/ru/company/press_releases.html.
176. https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/.
177. https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/whats-new-in-windows-defender-atp-fall-creators-update/?source=mmpc.
178. https://www.cnet.com/news/microsoft-build-smart-antivirus-using-400-million-computers-artificial-intelligence/.
179. Shi Y., Chng B., Kurtsiefer C. *Appl. Phys. Lett*., **109**, 041101 (2016).
180. Jennewein T. et al. *Rev. Sci. Instrum*., **71**, 1675 (2000).
181. Nie Y.-Q., Huang L., Liu Y., Payne F., Zhang J., Pan J.-W. *Rev. Sci. Instrum*., **86**, 063105 (2015).
182. Wayne M.A., Kwiat P.G. *Opt. Express*, **18**, 9351 (2010).
183. Symul T., Assad S.M., Lam P.K. *Appl. Phys. Lett*., **98**, 231103 (2011).
184. Xu F., Qi B., Ma X., Xu X., Zheng H., Lo H.-K. *Opt. Express*, **20** (11), 12366 (2012).
185. Kravtsov K.S. et al. *J. Opt. Soc. Am. B*, **32** (8), 1743 (2015); DOI: https://doi.org/10.1364/JOSAB.32.001743; https://www.osapublishing.org/josab/abstract.cfm?uri=josab-32-8-1743.
186. Rine D.C. (Ed.) *Computer Science and Multiple-Valued Logic: Theory and Applications* (Amsterdam, North Holland, 1984, Ch.7-9).
187. Шимбирев П.Н. *Гибридные непрерывно-логические устройства* (М.: Энергоатомиздат, 1990).
188. Conway J.H., Guy R. *The Book of Numbers* (New York: Springer-Verlag, 1996).
189. Ifrah G. *The Universal History of Numbers. FromPrehistory to the Invention of the Computer* (New York: John Wiley&Sons, 1999, vol. I).
190. Чижов И.В. *Вестник моск. ун-та*, **3**, 40 (2009).
191. Antipov A.L., Bykovsky A.Yu., Egorov A.A. *J. Rus. Laser Research,* **29** (4), 322 (2008).
192. Быковский А.Ю. *Кр. сообщ. физ. ФИАН*, **11**, 9 (2013).
193. Антипов А.Л., Быковский А.Ю., Егоров А.А., Компанец И.Н. *Радиотехника*, **8**, 97 (2008).
194. Быковский А.Ю., Рагер Б.Ю. В сб. *Труды XII-го Всероссийского совещания по проблемам управления ВСПУ-2014* (М.: ИПУ, 2014, с. 3917).
195. Bykovsky A.Yu., Sherbakov A.A. *J. Phys. Conf. Ser*., **737** (1), 12059 (2016).
196. Moiseev S.A., Skrebnev V.A. *Phys. Rev. A*, **91**, 022329 (2015); DOI: https://doi.org/10.1103/PhysRevA.91.022329; https://journals.aps.org/pra/abstract/10.1103/PhysRevA.91.022329.
197. Brassard G. *Modern Cryptology: A Tutorial, Lecture Notes in Computer Science* (New York: Springer, 1988, vol. 325).
198. Боумейстер Д., Экерт А., Цайлингер А. *Физика квантовой информации* (М.: Постмаркет, 2002).
199. Холево А.С. *Введение в квантовую информацию* (М.: МЦНМО, 2002).
200. Нильсен М., Чанг И. *Квантовые вычисления и квантовая информация* (М.: Мир, 2006).
201. Килин С. и др. *Квантовая криптография: идеи и практика* (Минск, Бел. наука, 2007).
202. Самарцев В.В. *Коррелированные фотоны и их применения* (М.: Физматлит, 2014).
203. Хренников А.Ю. *Введение в квантовую теорию информации* (М.: Физматлит, 2017).
204. Альбов А.С. *Квантовая криптография* (С.-Пб: Стратаб, 2016).
205. Жизан Н. *Квантовая случайность. Нелокальность, телепортация и другие квантовые чудеса* (М.: Альпина-нон фикшн, 2016).
206. Иванов М.Г. *Как понимать квантовую механику* (М.–Ижевск: НИЦ « Регулярная и хаотическая динамика», 2012).