Секция радиоэлектронных технологий и информационной безопасности

УДК 535.14

К.Е. Румянцев, И.Е. Хайров, В.В. Новиков

РАСПРЕДЕЛЕНИЕ СЕКРЕТНОГО КЛЮЧА В ОПТИЧЕСКИХ СЕТЯХ С КОЛЬЦЕВОЙ ТОПОЛОГИЕЙ МЕТОДАМИ КВАНТОВОЙ КРИПТОГРАФИИ

Идеи создания квантовых компьютеров и бурно развивающаяся в связи с этим квантовая информатика породили новое направление, получившее название квантовая криптография, основной задачей которого является защищенное распределение секретного ключа между пользователями.

При использовании квантово-криптографических методов генерация ключа может происходить непосредственно в процессе передачи по абсолютно открытому каналу. Носителями в данном случае являются элементарные частицы (фотоны), тот или иной физический параметр которых определяет полезную информацию. Надежность этих методов держится на нерушимости фундаментальных законов квантовой механики [1].

При теоретическом рассмотрении процесса обмена данными, когда передача осуществляется при помощи одиночных фотонов, криптоаналитик не может отвести себе часть сигнала, так как нельзя поделить электромагнитный квант на части. В реальных же условиях это вызовет сильное затухание сигнала (либо его полное отсутствие), что поставит под сомнение корректность приема получателем секретного ключа. При непосредственном вмешательстве в процесс обмена сильно возрастает уровень ошибок, и присутствие злоумышленника будет обнаружено легальными пользователями.

Большинство существующих практических квантово-криптографических систем обеспечивают обмен ключами только между двумя пользователями. В связи с этим одним из основных направлений исследований в квантовой криптографии является создание сетей распределения ключа между большим количеством пользователей. В настоящее время предложен ряд таких систем.

Методы квантовой криптографии могут использоваться при построении пассивной оптической сети, содержащей центральный сетевой контроллер А, связанный посредством пассивного оптического светоделителя с множеством сетевых пользователей $Б_i$. В этой схеме используется квантовое поведение оптического светоделителя. Одиночный фотон в светоделителе не может разделяться, а, напротив, направляется по одному из путей. Выбор пути для каждого отдельного фотона произволен и непредсказуем. Следовательно, если стандартный протокол квантовой передачи применяется в сети со светоделителями, то каждый пользователь будет обеспечен уникальным произвольно выбранным подмножеством битов. Из последовательности, которая передается в сети, центр А может, выполняя открытое обсуждение после передачи с каждым пользователем по очереди, идентифици-

ровать, какие фотоны были разделены с каждым из них, и создать с каждым секретный и уникальный секретный ключ. Таким образом, сеть может быть надежно защищена, так как центр А и пользователи $Б_i$ могут быть уверены, что никакой другой сетевой пользователь или внешний злоумышленник не получил никаких сведений относительно их общего ключа [2].

Подобный метод построения сети изображен на рис. 1,а. Отправитель Т связывается в квантовом канале с пользователями R1-R3. Пользователи могут быть расположены в узлах общей системы связи. Метод предполагает генерацию различных секретных ключей для каждого пользователя. Тактовые импульсы могут передаваться пользователям для синхронизации до начала передачи в квантовом канале. Квантовый канал может быть мультиплексирован, а передача в нем может осуществляться параллельно с классическим многофотонным обменом данных в сети [3]. Данный метод используется для реализации сети с древовидной топологией.

В системе связи с кольцевой топологией, использующей квантовую криптографию для распределения ключа, две станции независимо модулируют однофотонный сигнал (рис. 1,б). Этот однофотонный сигнал передается пользователям сети от внешнего источника и проходит через станции последовательно. Сигнал впоследствии проходит на третью станцию, которая определяет состояние сигнала и сравнивает его с первоначально переданным состоянием. Эта третья станция передает результаты сравнения на две станции, и они формируют общий секретный ключ для последующего шифрования информации. Передающая станция (Alice) может содержать помимо источника одиночных фотонов также и однофотонный детектор [4].

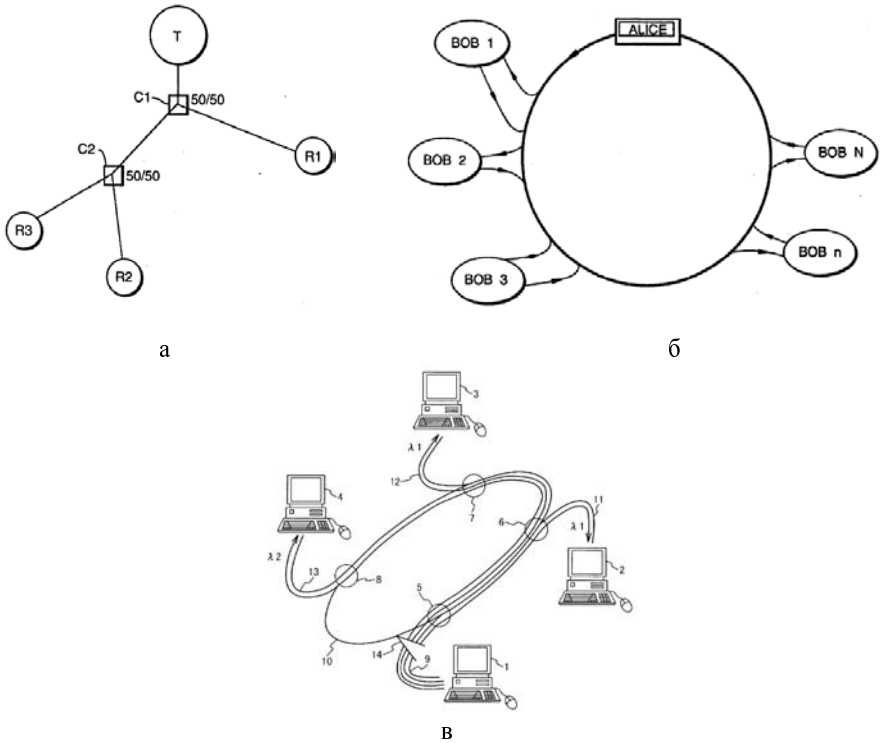

Рис.1. Распределение секретного ключа в оптических сетях, использующих методы квантовой криптографии

Другая квантово-криптографическая система содержит квантовый канал связи с множеством узлов, включающих передающий и приемный модули, связанные с квантовым каналом связи (рис. 1,в). Передающий модуль генерирует световой сигнал, представляющий собой последовательность фотонов, для распределения через квантовый канал. Промодулированное квантовое состояние фотонов передается получателю. Получатель сообщения принимает световой сигнал, посланный передатчиком, и измеряет квантовые состояния этого сигнала. Затем получатель определяет присутствие или отсутствие несанкционированного съема, основываясь на исходной и переданной квантовой последовательностях состояний и на измеренных квантовых состояниях. Данный метод организации оптической сети использует кольцевую топологию, однако основным ее достоинством является то, что каждый из пользователей может быть инициатором обмена данными [5, 6].

Также известен метод обмена информацией между большим количеством пользователей, основанный на квантовой криптографии. Этот метод отличается тем, что однофотонный сигнал от отправителя может быть немодулирован [7]. В этом случае каждый из пользователей произвольно выбирает один из множества алфавитов шифрования, который соответствует различным квантово-механическим операторам его детектора. Пользователи модулируют однофотонный сигнал с помощью выбранного оператора и возвращают его отправителю. Отправитель, в свою очередь, произвольно выбирает квантово-механический оператор и использует его для детектирования сигнала, возвращенного пользователем. Переданное и полученное состояния однофотонного сигнала сравниваются, с целью обнаружения несанкционированного доступа.

Все рассмотренные методы распределения секретного ключа используют либо древовидную топологию сети, либо кольцевую с необходимостью использования дополнительных каналов обмена информацией. В связи с этим актуальной и закономерной является проблема разработки метода распределения секретного ключа между большим количеством последовательно расположенных пользователей без дополнительных каналов обмена информацией. В работе предложен новый метод организации оптической сети, в которой происходит распределение секретного ключа с использованием квантовой криптографии. Данный метод основан на принципе измерение–повторная отправка и применим в системах с модуляцией по поляризации. Проанализировать работу сети можно предполагая, что процесс обмена данными происходит между тремя пользователями: пользователь А передает секретный ключ пользователю Б через пользователя В.

Исследования показали, что при непосредственном использовании данного метода процесс обмена характеризуется большим процентом ошибок. Однако с введением в рассматриваемую сеть подсистемы синхронизации между поляризационными анализаторами пользователей Б и В, данный метод будет соответствовать протоколам, применяющимся для обмена данными между несколькими пользователями (рис. 2).

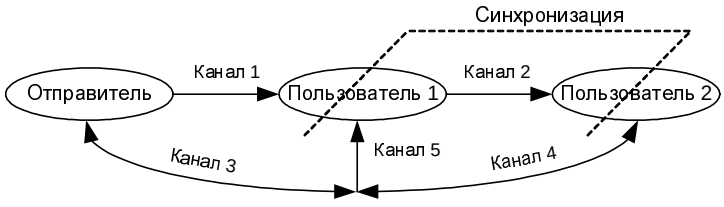

Рис.2. Процесс передачи секретной информации в оптической сети, использующей квантовые (1 и 2) и классические (3–5) каналы

Данная оптическая сеть распределения секретного ключа методами квантовой криптографии может быть также отнесена к сети связи с кольцевой топологией.

Основной проблемой практической реализации подобной оптической сети является обеспечение точной синхронизации поворотов поляризационных анализаторов большого количества последовательно расположенных пользователей. Так как вероятность прохождения поляризованного фотона через анализатор пропорциональна косинусу угла между направлением поляризации и осью анализатора, то неточность синхронизации может составлять единицы градусов.

Начальная установка приемопередающего оборудования не является решением проблемы синхронизации, так как ориентация анализаторов меняется случайным образом независимо от передающего модуля. В этом случае временная синхронизация также не применима, так как приводит к потере секретности. Злоумышленник, перехватив синхросигнал, может остаться незамеченным для авторизованных пользователей.

Необходимо также отметить, что описанный выше метод может быть использован для организации обмена данными между большим количеством последовательно расположенных пользователей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Румянцев К.Е., Хайров И.Е., Новиков В.В.* Доступ к информации, передаваемой по квантово-криптографическому каналу // Материалы электронной конференции “Приоритетные направления развития науки, техники и технологий”. РАЕ, 2004.
2. *Vakhitov A.V., Makarov V., Hjelme D.R.* Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography // Journal of modern optics. 2001. Vol. 48. №13. P. 2023–2038.
3. Патент 95/07582 GB, МКИ^6 H 04 L 9/08. Опубл. 16.03.95.
4. Патент 95/07585 GB, МКИ^6 H 04 L 9/08. Опубл. 16.03.95.
5. Патент 2003/0002674A1, США, МКИ^6 H 04 L 9/00. Опубл. 15.12.98.
6. Патент 2003/18144A, Япония, МКИ^6 H 04 L 9/00. Опубл. 17.01.2003.
7. Патент 005850441A, США, МКИ^6 H 04 L 9/00. Опубл. 15.12.98.

УДК 535.14

И.Е. Хайров, К.В. Клочко

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО СЪЕМА В СИСТЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ С КОДИРОВАНИЕМ ФОТОНОВ ПО ФАЗЕ

В последнее время интенсивно развивается одно из современных направлений квантовой информатики, получившее свое официальное название "квантовая криптография". Методами квантовой криптографии (КК) удается создавать абсолютно случайные секретные ключи между пользователями квантовой линии связи [1]. Одним из самых распространенных протоколов КК является протокол BB84, разработанный в 1984 году сотрудниками компании IBM Ч. Беннеттом и Г. Брассаром. В случае модуляции фотонов по относительной фазе данный протокол использует 4 фазовых состояния. При этом в зависимости от разности фаз однофотонных импульсов передающего и приемного модулей возможна конструктивная либо деструктивная интерференции, что определяет передаваемый бит информации.