СИСТЕМА ПЕРЕДАЧИ КЛЮЧА ШИФРОВАНИЯ на основе протокола квантовой криптографии

О.Горбадей, к.т.н., зав. кафедрой Белорусской государственной академии связи / post@bsac.by,
А.Зеневич, д.т.н., ректор Белорусской государственной академии связи / a.zenevich@bsac.by,
А.Соловьев, науч. сотр. Белорусской государственной академии связи / bsac@bsac.by

УДК 621.383, DOI: 10.22184/2070-8963.2022.106.6.60.63

Представлена реализованная система передачи секретного ключа, основанная на работе протокола квантовой криптографии BB84. Определены параметры и характеристики данной системы. Формируемые ключи проверены на случайность по стандартам NIST.

Введение

Для передачи данных в настоящее время наиболее широкое применение находят одномодовые оптические волокна (ОВ). При трансляции данных по волокну достаточно часто приходится обеспечивать конфиденциальность передаваемой информации. Сегодня наиболее эффективными способами защиты информации, передаваемой по ОВ, являются решения квантовой криптографии. Считается, что эти методы позволяют обеспечивать абсолютную защищенность информации, поскольку в основу их положены принципы квантовой механики.

Основным недостатком использования квантовой криптографии является низкая скорость передачи информации по волоконно-оптическому каналу. Это не позволяет широко использовать данные методы в системах защиты информации, поэтому необходима разработка новых способов передачи секретного ключа на основе протоколов квантовой криптографии, которые позволят увеличить скорость передачи и будут достаточно просты в реализации, не требуя применения прецизионного оборудования.

Система передачи ключа шифрования

Структурная схема разработанной системы передачи секретного ключа по ОВ на основе использования протокола квантовой криптографии BB84 представлена на рис.1.

Принцип работы данной системы заключается в реализации протокола квантовой криптографии BB84 с использованием четырех оптических волокон. Для этого случайным образом выбирается источник оптического излучения, который направляет излучение в соответствующее ему волокно. Фотоприемник подключается для регистрации оптического излучения также случайным образом.

К каждому из четырех задействуемых ОВ подключен только один фотоприемник. Секретный ключ формируется по совпадениям выбора источника оптического излучения и подключения фотоприемника.

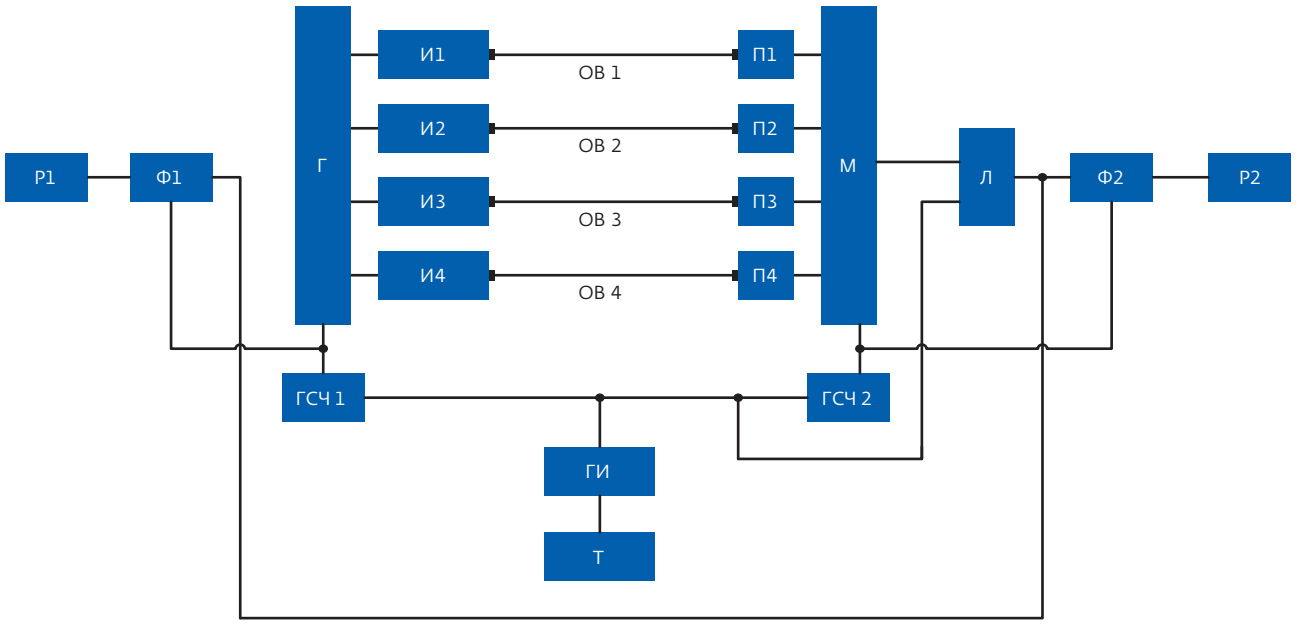

Рис.1. Структурная схема системы передачи секретного ключа по оптическому волокну: Т – таймер, ГИ – генератор тактовых импульсов, ГЧС1 и ГЧС2 – генераторы случайных чисел, Г – генератор, М – мультиплексор, Л – логический элемент "И", Ф1 и Ф2 – формирователи ключа, Р1 и Р2 – регистры, П1, П2, П3 и П4 – фотоприемники, И1, И2, И3 и И4 – источники оптического излучения, ОВ1, ОВ2, ОВ3 и ОВ4 – оптические волокна

Предлагаемая система передачи секретного ключа по оптическому волокну функционирует следующим образом. Время формирования секретного ключа задается таймером *Т*, показанным на рис.1. Для этого таймер вырабатывает импульс длительностью, соответствующей времени, необходимого для создания секретного ключа. Передний фронт этого импульса запускает генератор тактовых импульсов *ГИ*. Генератор тактовых импульсов синхронизирует между собой работу генераторов случайных чисел ГЧС1 и ГЧС2.

Генераторы ГЧС1 и ГЧС2 случайным образом вырабатывают числа из набора 1, 2, 3, 4. В зависимости от того, какое число поступит на управляющий вход генератора *Г*, на его выходе появляется электрический импульс с таким же номером. Этот импульс подается на соответствующий источник оптического излучения, в результате чего этот источник формирует оптический импульс, который поступает в оптическое волокно, подключенное к этому источнику.

В зависимости от того, какое число появится на управляющем входе мультиплексора *М*, к первому входу логического элемента "И" *Л* будет подключен выход фотоприемника с соответствующим номером. Вход этого фотоприемника при этом с помощью оптического волокна подключен к выходу соответствующего источника оптического излучения.

На выходе мультиплексора электрический сигнал появится только в том случае, когда к входу логического элемента окажется подключенным фотоприемник, номер которого совпадает с номером сработавшего источника оптических импульсов. Это произойдет, если в текущем такте работы устройства оба генератора случайных чисел сформируют один и тот же код.

Второй вход логического элемента "И" *Л*, как видно из рис.1, соединен с тактовым генератором импульсов *ГИ*. По приходу электрического импульса на второй вход логического элемента импульс с первого входа по открытой линии связи поступает на первые входы формирователей ключа *Ф1* и *Ф2*.

На второй вход формирователя *Ф2* поступает числовая последовательность от генератора ГЧС2. В зависимости от того, поступление какого числа на второй вход формирователя *Ф2* совпало с появлением импульса на его первом входе, в нем будет выработан логический нуль или логическая единица. После чего логический нуль или логическая единица передаются и записываются в регистр *Р2*.

Таблица 1. Сведения о количестве символов в массиве

Размер ключа, бит	Количество символов
128	5000
256	7000
512	9000

На второй вход формирователя *Ф1* поступает числовая последовательность от генератора ГЧС1. В зависимости от того, поступление какого числа на второй вход формирователя *Ф1* совпало с появлением импульса на его первом входе, в нем будет выработан логический нуль или логическая единица. После этого логический нуль или логическая единица передаются и записываются в регистр *Р2*.

Так при поступлении на второй вход единицы или тройки, а на первый вход электрического импульса формирователи *Ф1* и *Ф2* вырабатывают логический нуль. При поступлении на второй вход двойки или четверки, а на первый вход электрического импульса формирователи вырабатывают логическую единицу.

Таким образом, разработанная система позволяет формировать секретный ключ на основе протокола квантовой криптографии BB84 [1].

Параметры системы передачи секретного ключа

При создании системы передачи секретного ключа экспериментальным путем были подобраны количества символов в массиве, необходимые для формирования секретного ключа. Сведения о размерах массивов приведены табл.1.

Каждый из ключей, сформированных системой передачи секретного ключа, проверялся по стандартам NIST (National Institute of Standards and Technology) [2]. Проверка показала, что все они являются полностью случайными.

В процессе тестирования системы передачи секретного ключа были определены ее оптимальные характеристики. Сведения об этих характеристиках представлены в табл.2.

Значение скорости передачи данных, показанное в табл.2, соответствует случаю, когда протяженность оптических волокон, используемых в системе для передачи символов, отличается на 100 м друг от друга. Если это отличие сократить до 0,1 м, то удается достичь скорости передачи данных 5 Мбит/с. Такое увеличение скорости передачи позволяет сократить время формирования ключа до 0,03 с.

Для работы описанной системы была выбрана передача на длине волны 1310 нм. Использование данного номинала длины волны было связано с тем, что в этом окне прозрачности достаточно сложно обеспечить отвод излучения с ОВ без разрыва этого волокна [3]. Таким образом, применение данной длины волны позволяет повысить защищенность передаваемого ключа по сравнению с другими длинами волн, используемыми для трансляции данных по одномодовым оптическим волокнам.

Отметим, что в разработанной системе может использоваться любое одномодовое волокно. Однако для повышения защищенности передаваемых данных наиболее целесообразно использовать оптическое волокно типа G.657, поскольку данное волокно более устойчиво к изгибам. Под устойчивостью к изгибам понимается то, что такое ОВ имеет меньшее затухание оптической мощности в области изгиба по сравнению с одномодовыми волокнами других типов. Поэтому злоумышленнику реализовать канал утечки информации в области изгиба для такого волокна наиболее сложно.

Для системы передачи секретного ключа было разработано специальное программное обеспечение, позволяющее определять вероятность возникновения ошибки регистрации, а также корректировать ошибки, появляющиеся при передаче данных. Это ПО позволяет отслеживать изменение ошибки регистрации в случае ее превышения некоторого заданного значения прекращать передачу данных для формирования секретного ключа.

При передаче данных в системе вероятность ошибки регистрации превышала 10^{-4}, для обеспечения такой ошибки регистрации отношение

Таблица 2. Характеристики системы передачи секретного ключа

Скорость передачи данных, кбит/с	Максимальная дальность передачи ключа, км	Длина волны оптического излучения, нм	Вероятность ошибки регистрации	Время формирования ключа, с
300	50	1310	$>10^{-4}$	0,5

сигнал/шум должно быть более 10 дБ. Отметим, что при протяженности оптического волокна 50 км потеря мощности в нем составляла от 17 до 20 дБ в зависимости от используемого образца. Для приема оптического излучения использовались фотоприемники с пороговой чувствительностью –80 дБм. Поэтому средняя мощность источников оптического излучения составляла 50 дБм.

Для таких приемников и источников оптического излучения увеличение протяженности ОВ (дальности передачи ключа) более 50 км приводило к увеличению ошибки регистрации и снижению пропускной способности системы.

Заключение

Создана система передачи секретного ключа, работа которой заключается в реализации протокола квантовой криптографии BB84 с использованием четырех оптических волокон. При этом случайным образом выбирается источник оптического излучения, который направляет излучение в соответствующее ему оптическое волокно. Также случайным образом подключается для регистрации оптического излучения фотоприемник. Для этого к каждому из четырех оптических волокон подключен только один фотоприемник. Секретный ключ формируется по совпадениям выбора источника оптического излучения и подключения фотоприемника.

Определены характеристики системы передачи секретного ключа по четырем оптическим волокнам на основе протокола квантовой криптографии BB84.

Благодарность

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор № Т21 УКРГ-010).

Литература

1. **Бернет С., Пэйн С.** Криптография. Официальное руководство RSA Security. М.: Бином-Пресс, 2002. 384 с.
2. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800-22, Revision 1a. Gaithersburg: National Institute of Standards and Technology, 2010. 131 p.
3. **Хорошко Д.Б.** Квантовая криптография: индивидуальный перехват с учетом протокола коррекции ошибок // Квантовая электроника. 2007. Т. 37. № 12. С. 1105–1108.