Модель системы квантового распределения ключей по оптическому волокну с временным кодированием

С.Ю.Решетников, О.В.Косоногов

Научный руководитель: доктор физико-математических наук, заведующий кафедрой РЗИ профессор Задорин А.С.

Аннотация: Разработана и исследована программная модель системы квантового распределения ключей BB84 с временным кодированием по волоконно-оптическим линиям. Рассмотрены и частично реализованы блоки, гарантирующие защищенность ключа.

Ключевые слова: Квантовое распределение ключа, статистический контроль, интерферометрический контроль.

Постановка Задачи

Разработка оптоволоконного канала связи для передачи конфиденциальных данных на основе технологии квантовой криптографии.

Ведение

Квантовая криптография в нынешнее время является одним из перспективных направлений в системах шифрования данных. Она позволяет реализовать абсолютно секретную передачу данных между двумя пользователями линии связи.

Квантовое распределение ключей (КРК) решает основную проблему симметричного шифрования - генерацию двух идентичных реплик ключа у двух удаленных пользователей таким образом, что третья реплика этого ключа не может существовать в природе [1]. Однако, несмотря на абсолютную (теоретическую) невозможность скрытного перехвата квантового ключа, практическая реализация не дает безусловной защищенности ключа, т.к. не существует волоконно-оптических линий связи (ВОЛС) без затуханий и поглощений, идеальных источников однофотонных состояний (КОС) и др. [2]. В реальных системах защищенность ключа обеспечивается вводом дополнительных блоков обработки статистики уровня ошибок, скорости генерации ключа, распределения однофотонных состояний в квантовом канале и интерферометрическим контролем. В рассматриваемой ниже системе, ориентированной на работу с ВОЛС, наиболее распространен классический протокол BB84 с фазовым или временным кодированием КОС. Реализация протокола - BB84-ВК [1,3], при этом представляется наиболее доступной для построения экспериментальных моделей систем КРК.

Основная часть

В наиболее простом варианте в системе КРК, основанной на протоколе BB84-ВК, удаленные пользователи А и Б соединяются квантовым и классическим каналами связи [1,3]. По первому из них (ВОЛС) передаются КОС, а по второму - обсуждаются результаты корректной регистрации этих КОС

Для шифрования используется КОС, сдвинутое относительно синхроимпульса в каждой посылке на определённую величину, для кодирования битов “0” и “1”. Формируются 2 базиса и внутри каждого базиса по 2 подбазиса. Тайм слот разбивается на окна. Каждому окну присваивается значение “0” или “1” [4].

Для каждого базиса и подбазиса значения окна будут разные. Логическая схема приведена на рисунке 1 [5].

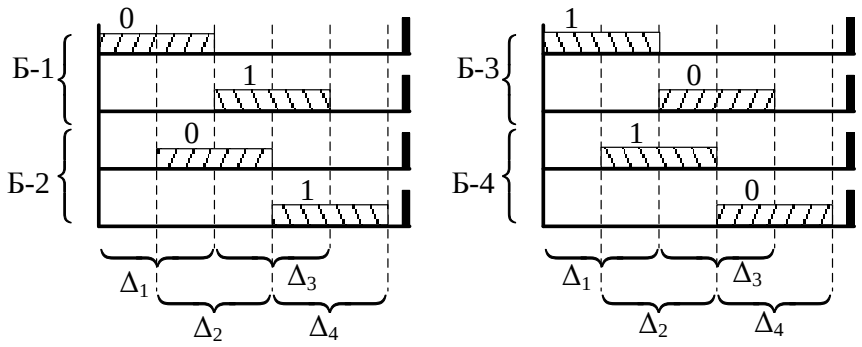

Рис.1 Кодовое состояние базисов и окон.

Б-i – базисные состояния, Δ_i – временные окна в пределах каждого из базисов.

На стороне А: для каждого тайм слота выбирается случайным образом с помощью генератора ПСП-1 базис и подбазис, в них соответственно также случайно с помощью генератора ПСП-2 выбирается значение бита, которое импульс фотона будет нести: “0” или “1”. Это выбранное значение и будет окном – сдвигом относительно синхроимпульса.

На стороне Б: аналогично для каждого тайм слота формируются базис и подбазис. Окна отсчитываются от момента появления синхроимпульса. Зная, в какое окно попал импульс фотона, известно какую информацию он нес: “0” или “1“. В конце тактового интервала по открытому каналу стороне А отправляются значения базиса и подбазиса для тайм слота, в котором был замечен импульс фотона, если базис с подбазисом совпадает, то сторона А по открытому каналу отправляет сигнал на запись и соответственно записывает в блокнот значение, которое нёс этот импульс фотона. Сторона Б поступает аналогично [4].

Модель системы разработана в пакете Matlab-Simulink, структурная схема, которой представлена на рисунке 2

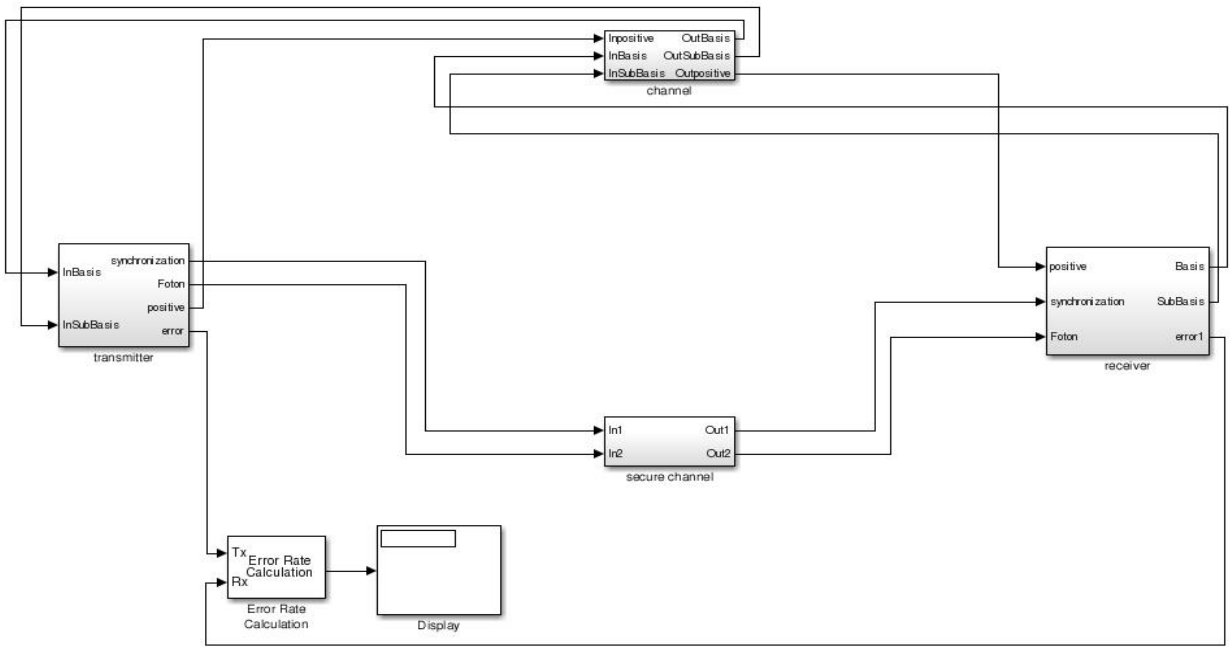

Рис. 2 Структурная схема модели.

На рисунке 3 представлена подробная схема передающей стороны. Здесь в соответствии свыше описанным алгоритмом представлены: блок формирования окон, блок формирования однофотонных состояний, блок записи и сравнения.

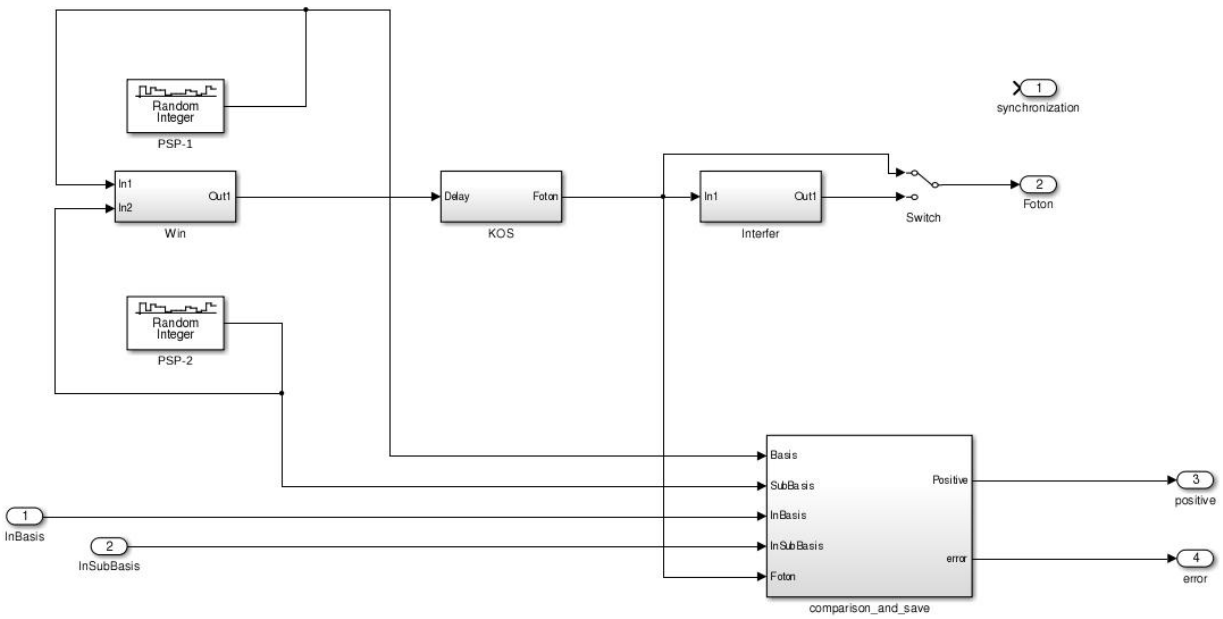

Рис. 3 Структурная схема пользователя А.

Излучения лазерных источников, которые генерируют свет в когерентном состоянии, характеризуются распределением Пуассона.

$$p(n,\lambda) = \frac{\lambda^{n} \cdot e^{-\lambda}}{n!} \quad (1)$$

Вместе с требующимися однофотонными импульсами всегда будут присутствовать пустые импульсы (n = 0) и многофотонные (n $\geq$ 2). Основной задачей является снижение вероятности появления многофотонных импульсов. Для этого среднее число фотонов в поле следует принимать за 0.1. Большее уменьшение среднего числа фотонов приведет к значительной доли пустых импульсов, что в свою очередь недопустимо уменьшит эффективную скорость передачи данных [6].

К контролируемым параметрам относится показатель вероятности ошибок P_f, скорость генерации секретного ключа B, и распределение описываемое формулой (1).

Считается, что защищенность ключа в системе обеспечивается до тех пор, пока P_f не превысит критического уровня $P_{fкр}$~11%. Контроль распределения заключается в проверке появления пустых (n = 0), однофотонных (n=1) и многофотонных (n $\geq$ 2) импульсов с последующим сравнением этих вероятностей с полученными значениями из формулы (1) [7]. Скорость генерации секретного ключа B можно рассчитать по формуле

$$B = B_0(1 - P_l)p(1,0.1)k_p 10^{-\frac{\alpha L}{10}} \quad (2)$$

где B_o – тактовая частота системы, k_p – коэффициент снижения скорости, предусмотренный конкретным протоколом КРК, L и α длина и погонное затухание ВОЛС соответственно; $p(n,\lambda)$ – вероятность генерации n-фотонной посылки в тактовом интервале, которая при среднем числе λ, описывается пуассоновской статистикой. P_l – вероятность пропуска сигнальных посылок [8]. Динамическое изменение этих трех параметров может указывать на возможные попытки взлома ключа, поэтому их мониторинг является важной задачей в обеспечение защищенности ключа.

Метод интерферометрического контроля основывается на включении интерферометра на обеих сторонах системы. Принцип действия интерферометра: пучок электромагнитного излучения (света, радиоволн и т.п.) с помощью того или иного устройства пространственно разделяется на два или большее количество когерентных пучков. Каждый из пучков проходит, различные оптические пути и возвращается на экран, создавая интерференционную картину, по которой можно установить смещение фаз пучков.

В данной системе структура интерферометра будет заключаться в следующем: на входе устройства под некоторым углом располагается неглухое полупрозрачное зеркало, способное с равными вероятностями пропустить фотон по одному из двух имеющихся каналов, различных по длине; на более длинном канале установлен фазовращатель, на выходе устройства также под определённым углом установлено неглухое полупрозрачное зеркало, объединяющее два различных по длине канала.

В результате использования интерферометров на выходе системы будет наблюдаться интерферометрическая картина фотонного импульса. При наличии прослушки канала интерферометрическая картина изменится, станет более нечёткой, расплывчатой [6,9].

Заключение

Модель системы квантового распределения ключей BB84-BK не является достаточно надежной, для обеспечения безусловной защищенности требуется вводить дополнительные блоки статистической обработки, интерферометрический контроль. Дальнейшие исследование будут проводиться в направлении реализации интерферометрического контроля, моделирования все возможных атак на систему: PNS-атака (Photon Number Splitting), UM-атака (Unambiguous Measurements) и др, адекватного поведения системы в случае детектирования атак с последующей практической реализацией системы КРК.

Список использованных источников

1. С.Н. Молотков Квантовая криптография и теоремы В. А. Котельникова об одноразовых ключах и об отсчетах.//УФН, 176:7 (2006), 777–788 с.;
2. Первая компьютерная сеть защищена на квантовом уровне [Электронный ресурс].- Режим доступа http://www.securitylab.ru/news/213933.php;
3. С. Н. Молотков Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы / С. Н. Молотков // Письма в ЖЭТФ. — 2004.— Т. 79.— С. 691–704
4. Румянцев К. Е., Голубчиков Д. М. Квантовая связь и криптография: Учебное пособие. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – 122 с.;
5. Задорин А.С., Махорин Д.А. Модель системы квантового распределения ключей по оптическому волокну с временным кодированием / Журнал "Доклады Томского государственного университета систем управления и радиоэлектроники" № 3 (33), 2014 год, стр. 85–89.
6. Килин С.Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. – 2008. - 391с.;
7. С.Н. Молотков О предельных возможностях квантового распределения ключей с контролем статистики неоднофотонного источника//Письма в ЖЭТФ, 87:10 (2008), 674–679 с.;
8. Е.И. Куликов Прикладной статистический анализ М.: Горячая линия-Телеком, 2008 464 с.;
9. Имре Б. Балаж Ф. Квантовые вычисления и связь. Инженерный подход / Пер. с англ. под ред. В.В. Самарцева. – М.: ФИЗМАТЛИТ, 2008. – 320 с.