УДК 621.383.523

А.С. Задорин, Д.А. Махорин

Модель системы квантового распределения ключей по оптическому волокну с временным кодированием

Разработана и исследована программная модель системы квантового распределения ключей BB84 с временным кодированием по волоконно-оптическим линиям. Исследована зависимость ошибок генерации ключа от шумов системы и порога компаратора ФПУ. Рассмотрены возможности усиления защищенности протокола за счет статистического мониторинга ключевых параметров системы.

Ключевые слова: квантовое распределение ключей, скалярный контроль статистики квазиоднофотонных состояний.

Развитие технологий квантовых вычислений и квантовых процессоров, реализующих генерацию в т.ч. одного из важнейших криптографических примитивов – квантовое распределение ключей (КРК), как известно, позволяет решить основную проблему систем электронного симметричного шифрования – формирование в режиме «одноразового блокнота» удаленными пользователями А и Б, расположенными на обеих сторонах канала КРК, идентичных копий секретного ключа. За прошедшие полтора десятилетия было предложено и исследовано большое число протоколов КРК, разработаны первые коммерческие квантовые криптосистемы [1–4]. Известное доказательство безусловной защищенности от внешних атак генерируемого таким образом ключа, строго говоря, распространяется лишь на идеальные системы, в которых все сигнальные квантовые состояния являются строго однофотонными, в канале связи отсутствуют поглощение и шумы, а квантовая эффективность фотодиода приемника составляет 100%. Тем не менее безусловная защищенность ключа может обеспечиваться и в реальных системах. Осуществляется это за счет усиления протоколов КРК комбинациями контроля нескольких параметров даже не строго однофотонных состояний, а приготавливливаемых путем простого ослабления лазерного излучения [5]. Ниже такие состояния будем называть квазиоднофотонными состояниями (КОС). Известно, что защищенность ключа в указанных системах обеспечивается до тех пор, пока уровень ошибочных символов в репликах ключа на обеих сторонах канала связи (P_f) не превысит некоторой критической величины $P_{f\_кр}$. Уровень $P_{f\_кр}$ ограничивает длину линии $L_с$ и зависит от используемого протокола КРК [6]. В рассматриваемых ниже системах, ориентированных на работу с волоконно-оптическими линиями связи (ВОЛС), наиболее распространен классический протокол BB84 с фазовым или временным кодированием КОС. Реализация последнего варианта протокола – BB84-ВК [7, 8] – при этом представляется наиболее доступной для построения экспериментальных моделей систем КРК.

Целью настоящей работы является изучение особенностей использования BB84-ВК в системах КРК с ВОЛС, моделирование работы системы в пакете Matlab-Simulink, а также исследование возможностей усиления протокола за счет контроля статистики КОС на приемной стороне системы.

Система КРК на основе BB84-ВК. В наиболее простом варианте в системе КРК, основанной на протоколе BB84-ВК, удаленные пользователи А и Б соединяются квантовым и классическим каналами связи. По первому из них (ВОЛС) передаются КОС, кодируемые временными сдвигами относительно границ тактовых интервалов в пределах фиксированного набора базисов, а по второму - обсуждаются результаты корректной регистрации этих КОС [7]. Предполагается, что защита квантового канала указанной системы от атак, осуществляемых агентом Е, должна гарантироваться теоремой о запрете клонирования (ТЗК) неортогональных КОС, обеспечиваемых соответствующим временным сдвигом окон в применяемых базисах.

В рассматриваемом варианте КРК-BB84-ВК условия применимости ТЗК трудновыполнимы, т.к. при КОС-ВК агент Е не связан необходимостью коммутации протокольных базисов и окон. В условиях, например, когда длительность КОС меньше длительности базисного окна T, агент Е получает прямую возможность клонирования КОС, кодовое состояние которого он позднее легко установит в результате прослушивания классического канала связи. Эффективными в данных условиях могут

быть также атаки с измерениями с определенным исходом – UM-атаки (Unambiguous Measurements), а также PNS-атаки (Photon Number Splitting) [5]. Применение фазовых матриц (AWG) на входе ВОЛС [9] для выравнивания τ и T не может радикально устранить риск взлома ключа.

Больший уровень защищенности систем КРК-BB84-BK обеспечивает введение в них блоков контроля статистики КОС или блоков генерации и обработки состояний-ловушек (decoy states), реализуемых чаще всего на основе оптических интерферометров [6, 10, 11]. Интерферометрическая обработка состояний-ловушек значительно усиливает защищенность КРК, прежде всего за счет учета фазовых состояний КОС при их обработке. Однако высокий уровень защищенности систем КРК-BB84-BK от перечисленных выше атак агента Е может достигаться и при более простой, скалярной (без интерферометра) статистической обработке КОС на стороне пользователя Б.

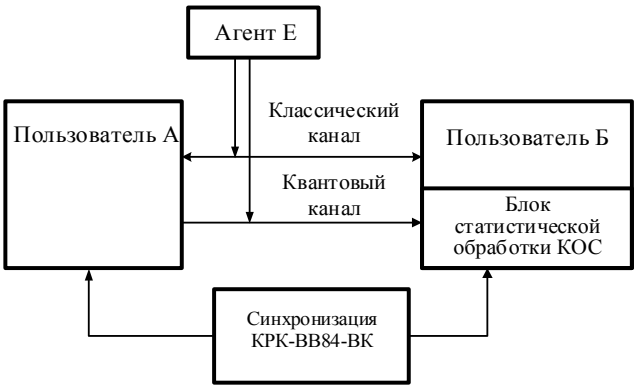

Рис. 1. Структурная схема КРК-BB84-BK

Рассмотрим разработанную нами модель такой системы, структурная схема которой представлена на рис. 1.

В качестве протокола взаимодействия пользователей А и Б для схемы рис. 1 нами был взят несколько измененный вариант оригинального протокола [7]. Логическая схема протокола приведена на рис. 2. Здесь изображен один тактовый интервал, в пределах которого показаны различные возможные кодовые состояния КОС. Вертикальной жирной меткой на каждом рисунке обозначены тактовые синхроимпульсы. Символами Б-*i* слева на рис. 2 пронумерованы базисные состояния КОС, а символами Δ_i снизу отмечены временные окна в пределах каждого из базисов. Введенные нами изменения касались устранения дополнительных окон в базисе 1 для символа «0» и в базисе 3 для символа «1», а также замена значений символов в окнах базиса 3 на противоположные. Введенные изменения были предприняты для обеспечения равной вероятности появления символов «0» и «1» в каждой точке тактового интервала.

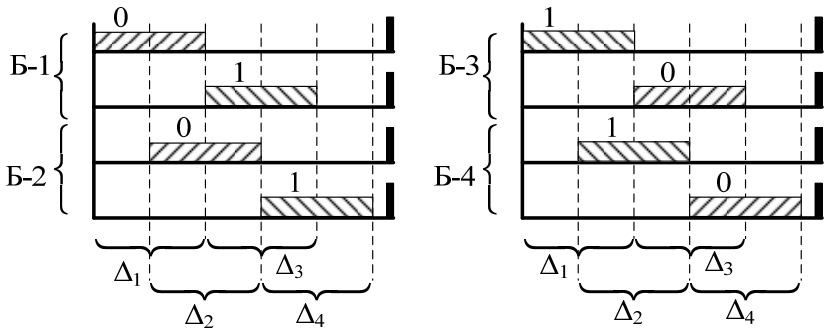

Рис. 2. Кодовые состояния базисов и окон протокола BB84-BK

Данное в [7] описание этапов реализации алгоритма генерации «просеянного» ключа применимо и для схемы рис. 2.

Более подробно структура программной модели пользовательского блока А, реализованная нами в пакете Matlab-Simulink, показана на рис. 3. Здесь, в соответствии с названым алгоритмом, генераторами псевдослучайных последовательностей ПСП 0-1 и ПСП Δi задаются значения символов КОС и код временного окна Δi. Для каждой пары сгенерированных чисел в дешифраторе рассчитывается соответствующий код временного базиса первого пользователя Б-*i*, который по классическому каналу пересылается для сравнения с кодом базиса второго пользователя Б.

Приемная часть аппаратуры пользователя Б содержит узлы, идентичные вышеназванным. При этом генераторы ПСП 0-1 и ПСП Δ_i приемной стороны не синхронизированы с соответствующими генераторами передатчика. Кроме этого, для обеспечения конфиденциальности состояний принятых КОС сигнал о совпадении базисов передается вторым пользователем не сразу, а в конце тактового интервала. Графический S-код обработки сигнала совпадения приведен на рис. 4.

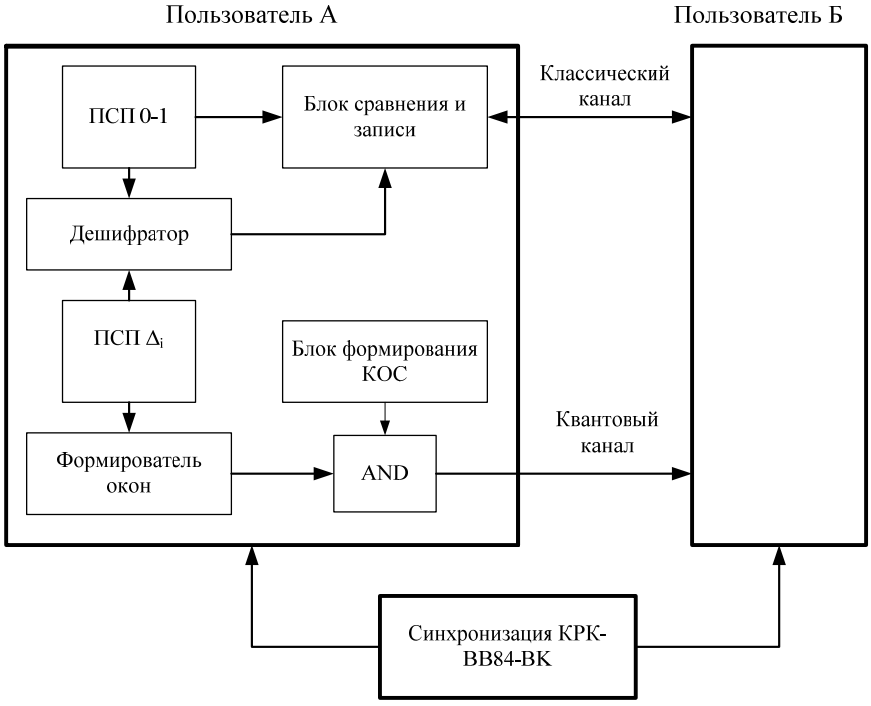

Рис. 3. Структура программной модели для пользователя А

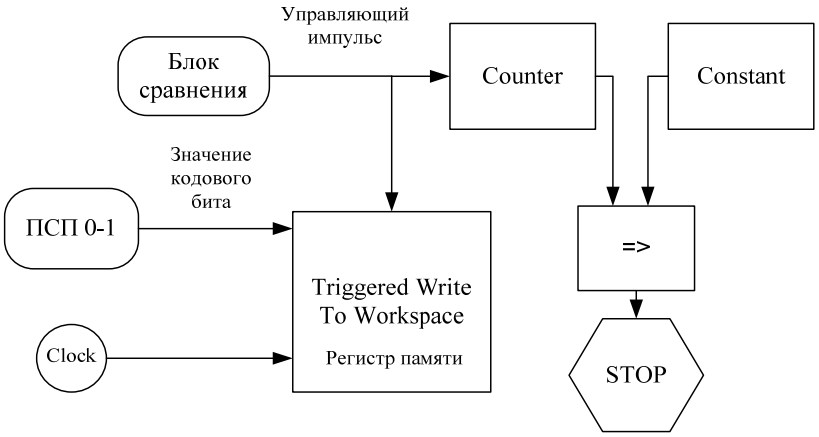

Рис. 4. Структура блока записи

Обработка, т.е. собственно генерация «просеянного» ключа (КП), сводилась к сверке пользовательских базисов и записи соответствующих состояний КОС в регистры памяти на обоих концах системы. Компонент Clock при этом фиксировал моменты времени срабатываний компараторов инициирующих запись элементов массивов ключа $КП_А$ и $КП_Б$ в соответствующие регистры памяти пользователей А и Б. Объем файла ключа КП при этом задавался параметрами блока Constant.

Разработанная модель использовалась для измерения вероятности генерации ложных символов P_f ключа, определяющей уровень ошибок системы, в отсутствие и при наличии белых гауссовых шумов фотоприемного устройства (ФПУ) и канала связи. Модельные эксперименты показали, что ошибочные символы в массивах $КП_А$ и $КП_Б$ возникают лишь при наличии шумов в системе. Усредненные по 10 выборкам расчетные зависимости P_f от уровней шума системы и порога U_0 компаратора ФПУ, нормированного к средней амплитуде *a* отклика приемника на одиночной КОС, показаны на рис. 5.

Цифрами *1* и *2* на рис. 5 отмечены кривые $P_f(U_p)$, измеренные при различных среднеквадратичных амплитудах шумового напряжения $U_ш$ на входе компаратора ФПУ, нормированного относительно *a*. В первом случае $U_ш = 0{,}15$, а во втором – $U_ш = 0{,}45$. Из представленных графиков хорошо видна возможность удержания допустимого системных ошибок на уровне ~11% с помощью регулировки порога ФПУ U_p.

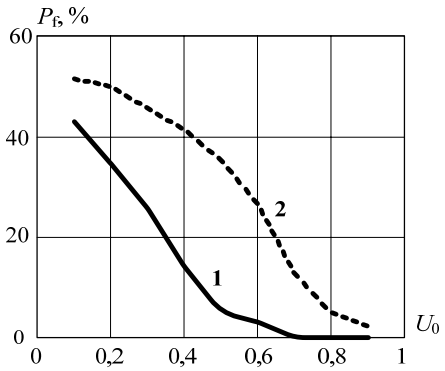

Рис. 5. Зависимость вероятности P_f от порога компаратора ФПУ U_0

Следует заметить, что повышение U_0 хотя и способствует снижению ошибок P_f, но одновременно с вероятностью P_l, приводят к пропускам сигнальных посылок в моменты опроса пороговой схемы и снижению скорости B генерации массива КП [12]

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

где B_o – тактовая частота системы; k_p – коэффициент снижения скорости, предусмотренный конкретным протоколом КРК; L и α – длина и погонное затухание ВОЛС соответственно; $p(n)$ – вероятность генерации n-фотонной посылки в тактовом интервале, которая при среднем числе КОС m описывается пуассоновской статистикой [13]:

$$p(n) = \frac{(m\cdot\eta)^n e^{-m\cdot\eta}}{n!}. \quad (2)$$

Вероятности P_l и P_f выражаются через плотности вероятности шума $p_n(n)$ и смеси сигнала с шумом $p_c(n)$ как [13]

$$P_l = \int_{-\infty}^{U_0} p_c(n)dn, \; P_f = \int_{-U_0}^{\infty} p_n(n)dn, \quad (3)$$

где U_0 – порог срабатывания ФПУ, выраженный через n.

Зависящие от $U_ш$, U_p, $p(1)$, k_p параметры B, P_f, вместе со статистическим распределением состояний КОС $p(n)$, являются основными системными показателями. Динамическое изменение этих параметров может указывать на возможные попытки взлома ключа, поэтому их непрерывный мониторинг является одной из задач блока контроля статистики системы рис. 1. Измерение средней скорости приема КОС B и распределения $p(n)$ при этом проводится путем непосредственных измерений состояний КОС на приемной стороне квантового канала. Следует заметить, что для контроля $p(n)$ пригодны лишь фотодиоды, работающие в линейном режиме, например лавинные фотодиоды (APD), чувствительность которых, ограниченная флуктуацией коэффициента умножения M, темновым током и др., может обеспечивать режим счета одиночных фотонов [14].

Уровень же ошибок P_f оценивается пользователями путем периодического обмена частью ключей $КП_А$ и $КП_Б$ по классическому каналу.

Заключение. Изложенные выше результаты показывают возможность создания системы КРК на основе протокола BB84-BK для ВОЛС, а также возможности усиления защищенности протокола за счет скалярного статистического мониторинга ключевых параметров системы.

Работа выполнена в рамках государственного задания №2406 от 21.02.2014 г.

Литература

1. Бауместер Д. Физика Квантовой Информации / Д. Бауместер, А. Экерт, А. Цайлингер. – М.: Постмаркет, 2002. –376 с.

2. Молотков С.Н. Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах // Успехи физических наук. – 2006. – Т. 176, вып. 7. – С. 777–788.

3. Килин С.Я. Квантовая криптография: идеи и практика / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. – Минск: Белорусская наука, 2008. – 392 с.

4. Первая компьютерная сеть защищена на квантовом уровне [Электронный ресурс]. – Режим доступа http://www.securitylab.ru/news/213933.php свободный (дата обращения: 10.07.2014).

5. Молотков С.Н. О решении проблемы обеспечения стойкости квантовой криптографии для канала связи со сколь угодно большой длиной // Письма в ЖЭТФ. – 2011. – Т. 93, вып. 12. – С. 830–836.

6. Молотков С.Н. О предельных возможностях квантового распределения ключей с контролем статистики неоднофотонного источника // Письма в ЖЭТФ. – 2008. – Т. 87, вып. 10. – С. 674–679.

7. Молотков С.Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // Письма в ЖЭТФ. – 2004. – Т. 79. – С. 691–704.

8. Debuisschert T. Time coding protocols for quantum key distribution / T. Debuisschert, W. Boucher // Physical Review A. – 2004. – Vol. 70, iss. 4. – P. 042306.

9. Молотков С.Н. К вопросу об обосновании квантовой криптографии на временных сдвигах // Письма в ЖЭТФ. – 2004. – Т. 80, вып. 7. – С. 576–582.

10. Hwang W.-Y. Quantum key distribution with high loss: Toward global secure communication // Phys. Rev. Lett. – 2003. – Vol. 91. – P. 057901.

11. Хорошко Д.Б. Квантовое распределение ключа на временных сдвигах с использованием состояний-ловушек / Д.Б. Хорошко, Д.И. Пустоход, С.Я. Килин // Оптика и спектроскопия. – 2010. – Т. 108, вып. 3. – С. 372–379.

12. Скорость генерации кода в системе квантового распределения ключей / А.С. Задорин, А.В. Максимов, Д.А. Махорин и др. // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 2. – С. 139–141.

13. Куликов Е.И. Прикладной статистический анализ. – М.: Горячая линия-Телеком, 2008. – 464 с.

14. Махорин Д.А. Возможность реализации линейного режима счета фотонов на лавинном фотодиоде S8664-05K при комнатной температуре / Д.А. Махорин, А.Б. Галиев, А.С. Задорин // Доклады ТУСУРа. – 2014. – № 1 (31). – С. 65–68.

Задорин Анатолий Семенович
Д-р физ.-мат. наук, профессор, зав. каф. радиоэлектроники и защиты информации (РЗИ) ТУСУРа
Тел.: 8 (382-2) 41-33-65
Эл. почта: Anatoly.Zadorin@rzi.tusur.ru

Махорин Дмитрий Алексеевич
Аспирант каф. РЗИ
Тел.: 8-913-824-11-11
Эл. почта: mda.tomsk@gmail.com

Zadorin A.S., Makhorin D.A.

Model of quantum key distribution system over optical fiber with time coding

The authors developed and investigated a software model of BB84 quantum key distribution with time-coded fiber optic lines. We studied the dependence of the error key generation systems and noise-threshold comparator UPF. We analyzed the opportunity for strengthening the security protocol at the expense of statistical monitoring of key system parameters.

Keywords: quantum key distribution, scalar control statistics quasi-photon states.
