УДК 621.383.523

А.С. Задорин, Д.А. Махорин

Статистическая обработка сигналов в системах квантового распределения ключей

Предложена модель усиления протокола квантового распределения ключей (КРК) за счет мониторинга статистики уровней ошибок, скорости генерации ключа и распределения квазиоднофотонных состояний в квантовом канале. Установлены границы безопасных зон работы квантового канала для различных типов атак.

Ключевые слова: система квантового распределения ключей, зоны безопасной генерации ключа, PNS-атака.

На развитие методологии построения безусловно защищенных систем конфиденциальной связи в последние полтора десятилетия заметное влияние оказали идеи использования квантовых объектов для генерации секретного ключа удаленными пользователями А и Б [1–3]. Системы, построенные на этих идеях, в литературе принято называть системами квантового распределения ключей (КРК) [4–6]. Безусловная секретность генерируемых системами КРК ключей основана, как известно, на фундаментальных запретах квантовой механики на копирование неортогональных состояний квантовых объектов, в качестве которых, как правило, предполагается использование одиночных фотонов оптического диапазона волн. Детектирование попыток подслушивания в таких системах обеспечивается за счет динамического мониторинга нескольких показателей – вероятности ошибок P_f, скорости генерации первичного ключа B, а также распределения вероятности числа фотонов $p(n)$ в сигнальных посылках. При этом абсолютный уровень криптозащищенности указанных систем гарантируется лишь для идеализированных условий – переноса сигналов по квантовому каналу строго одиночными фотонами, а также отсутствия шумов и потерь в канале связи.

В реальных условиях техника приготовления однофотонных состояний, как правило, сводится к ослаблению лазерного импульсов до уровня, характеризуемого средним числом фотонов m. При такой технологии распределение $p(n)$ значительно отклоняется от идеальной δ-функции и описывается пуассоновской статистикой [7]

$$p(n)=\frac{e^{-m}}{n!}m^n. \qquad (1)$$

Соотношение (1) показывает, что указанным способом приготовить идеальные однофотонные посылки не представляется возможным. Можно лишь с помощью параметра m регулировать вероятность их появления в сигнальном импульсе. В дальнейшем стохастические состояния фотонных посылок в квантовом канале, описываемые соотношением (1), будем называть квазиоднофотонными состояниями (КОС).

Вместе с отмеченным различием (1) от $\delta(n)$, для реального квантового канала характерно ненулевое значение погонного затухания линии α_0, а также ограниченный уровень квантовой эффективности η фотоприемного устройства (ФПУ).

Несмотря на нарушения всех названных выше теоретических условий криптоустойчивости протоколов КРК, их безусловная защищенность может обеспечиваться и в реальных системах [8, 9]. Возможность такого усиления протокола основана на контроле сразу всех параметров КОС, искажаемых при возможных атаках некого агента Е на квантовый канал системы КРК, а также за счет дополнения протокольных состояний КОС специальными состояниями-ловушками (decoy states-D-состояние) [9–11]. Указанные D-состояния формируются пользователем А путем динамического расщепления однофотонных состояний в разбалансированном интерферометре Маха–Цендера (ИМЦ). Таким образом, создается возможность не только простого статистического подсчета числа состояний-ловушек на обоих концах канала, но также и контроля фазовых соотношений между фрагментами расщепленного D-состояния, осуществляемого путем интерференционных измерений в ИМЦ.

К основным контролируемым скалярным параметрам системы КРК относятся P_f, B, а также распределение $p(n)$. Считается, что защищенность ключа в указанных системах обеспечивается до тех пор, пока P_f не превысит критического уровня P_{fkp}~11%, зависящего от скорости генерации ключа системой B, используемого протокола КРК длины L и шумов P_n квантового канала [9, 12].

Последний параметр удобно выразить через P_f и другой системный показатель P_l – вероятность пропуска сигнальных КОС на приемной стороне квантового канала. Для этого обозначим порог срабатывания компаратора ФПУ как U_0, выразим его через n, а P_n выразим через плотности вероятности шума $p_n(n)$ и смеси сигнала с шумом $p_c(n)$ [7]. Тогда

$$P_l = \int_{-\infty}^{U_0} p_c(n)dn, \quad P_f = \int_{-U_0}^{\infty} p_n(n)dn\,. \tag{2}$$

Скорость генерации системой КРК секретной ключевой последовательности (КП) B будет выражаться через введенные выше параметры P_l, L и α_0 как [14]

$$B = B_0(1-P_l)\,p(1)k_p 10^{-\frac{\alpha L}{10}}, \tag{3}$$

где B_o – тактовая частота системы; k_p – коэффициент снижения скорости, предусмотренный конкретным протоколом КРК.

Формулы (1)–(3), дополненные шумовой моделью ФПУ системы [13], позволяют рассчитать двумерную зависимость $B(P_f, \alpha_0 L)$. Пример расчета такой поверхности дан на рис. 1. Здесь шаг изменений аргументов по оси αL составляет 2,5 дБ, а по оси P_f – 3%. График получен для m = 0,1 и ФПУ, рассчитанного на работу с ЛФД S8664-05K в линейном режиме с коэффициентом лавинного размножения 100 и темновым током $0{,}15\times10^{-9}$ А.

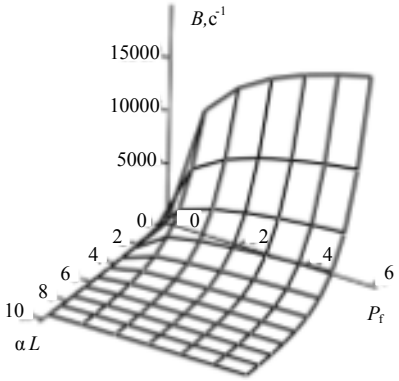

Рис. 1. Зависимость скорости генерации ключа от P_f и ослабления КОС в канале связи

С помощью $B(P_f, \alpha_0 L)$ можно установить безопасные для конкретных видов атак агента Е границы значений скорости генерации КП B и длины квантового канала L. Отыскание данных границ и является целью настоящей работы.

Границы безопасного режима систем КРК. Рассмотрим классическую систему КРК с источником КОС, описываемым формулой (1). Как отмечалось выше, использование подобного рода неидеальных источников сопряжено с рисками реализации нескольких видов атак [8, 9, 12]. Наиболее опасные из них – PNS-атака (Photon Number Splitting), UM-атака (Unambiguous Measurements) и др. – связаны с переконфигурированием агентом Е квантового канала, а также различного рода сортировок транслируемых по нему КОС. В ходе этих сортировок из пользовательских КОС в канале целиком или полностью исключаются однофотонные состояния, что приводит к изменению статистик $p_n(n)$ и $p_c(n)$. Естественно, что для обеспечения скрытности своей процедуры агенту Е необходимо сохранить значения строго контролируемых легитимными пользователями параметров B и P_f. Из формул (1)–(3) следует, что для этого достаточно изменить значения длины и погонного затухания квантового канала. Для отыскания этих значений пометим их штриховыми индексами (α' и L') и подставим в (1)–(3). Получим общую систему уравнений для L' и α':

$$\begin{cases} \left(1-P_l(L')\right)p(n')\cdot 10^{-\frac{\alpha' L'}{10}} = \left(1-P_l(L)\right)p(1)\cdot 10^{-\frac{\alpha L}{10}}, \\ P_f(L') = P_f(L). \end{cases} \tag{4}$$

Здесь $p(n')$ – вероятности измененных в ходе атаки КОС.

Связь уравнений в системе (4) определяется критериями (2) сортировки гипотез о наличии или отсутствии КОС в моменты опроса компаратора ФПУ, т.е. соответствующим пороговым уровнем U_0 и распределениями $p_n(n)$, $p_c(n)$.

В случаях, когда шумами в квантовом канале можно пренебречь, т.е. мощность шума P_n можно считать сосредоточенной на входе ФПУ пользователя Б,

$$P'_f(L') = P_f(L),\ P'_l(L') = P_l(L), \tag{5}$$

уравнение (4) линеаризуется и сводится к элементарному виду:

$$\alpha' L' = \alpha L - \left[\lg\left(m(1)\right) - \lg\left(m(n')\right)\right]. \quad (6)$$

Из (6) следует, что агент Е получает необходимый для маскировки бюджет ослабления

$$\Delta\alpha L = \alpha L - \alpha' L'$$

КОС в квантовом канале лишь тогда, когда ослабление основного канала (αL) превысит критический уровень $(\alpha L)_{кр}$:

$$(\alpha L)_{кр} = \left[\lg\left(m(1)\right) - \lg\left(m(n')\right)\right]. \quad (7)$$

Последнее соотношение вместе с (3) определяют безопасную нижнюю границу $B_{кр}$ скорости генерации системой ключевой последовательности, необходимую для обеспечения мониторинга статистической обработки КОС. Так, превышение текущего значения B уровня $B_{кр}$ означает, что агент Е не располагает необходимым для организации конкретного вида атаки бюджетом ослабления $\Delta\alpha L$.

Условие (5), определяющее границы применимости (6), можно считать выполненным, например, в квантовом канале, построенном на основе волоконно-оптической линии связи (ВОЛС). Однако в другом важном для практики случае атмосферного канала указанное условие не выполняется. Здесь с увеличением его длины L имеет место накопление фонового рассеяния. В ФПУ фоновое излучение вызывает избыточный дробовой шум, снижающий помехоустойчивость системы. В данных условиях границы безопасной зоны $(\alpha L)_{кр}$ необходимо отыскивать из решения нелинейного уравнения (4).

Рассмотрим, например, возможности организации PNS-атаки по ВОЛС. Как известно [8, 9, 12], данная атака сводится к тому, что агент Е неразрушающим образом измеряет в разрыве квантового канала числа фотонов в импульсах КОС. Однофотонные импульсы при этом блокируются, а пользователю Б транслируются только импульсы с двумя и более фотонами, один из которых агент Е сохраняет в своей квантовой памяти. Битовое состояние этого фотона агент Е может легко установить позднее, после раскрытия и согласования пользователями состояний соответствующих поляризационных базисов по классическому каналу.

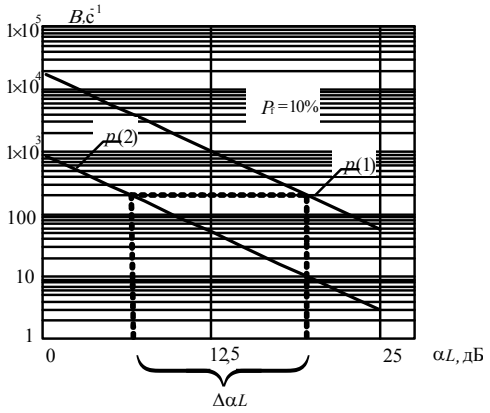

Рис. 2. Зависимость B от ослабления одно- и двух-фотонных КОС в ВОЛС

Для определения критического затухания в случае PNS-атаки учтем, что $p(n') = p(2)$, тогда из (6) получим $(\alpha L)_{кр} \sim 12{,}5$ дБ. Этот результат можно получить и прямым расчетом B по формуле (3). Соответствующие графики для параметров ФПУ к рис. 1, приведены на рис. 2.

Из рис. 2 видно, что необходимый для организации PNS-атаки бюджет ослабления в данных условиях составляет $(\alpha L)_{кр} = \Delta\alpha L \sim 12{,}5$ дБ, а уровень $B_{кр} \sim 1$ Кбит/с.

Заключение. Анализ приведенной выше модели системы КРК показывает, что усиление протокола за счет мониторинга статистики P_f, B и распределения $p(n')$ и установления границ $B_{кр}$ и $(\alpha L)_{кр}$ безопасных зон работы квантового канала для различных типов атак связано с учетом соответствующих статистик $p(n)$, $p_n(n)$ и $p_c(n)$ в формулах (1)–(7).

Из этих же соотношений видно, что использование в системах КРК традиционных лазерных источников с пуассоновской статистикой приготовления КОС, значительно увеличивает риски организации атак на генерируемый ключ и существенно снижает скорость этой генерации.

Литература

1. Quantum cryptography: Public key distribution and coin tossing [Электронный ресурс]. – Режим доступа http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf свободный (дата обращения: 27.07.2014).

2. Bennett C.H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. – 1992. – Vol. 68, № 21. – P. 3121.

3. Ekert A. Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. – 1991. – Vol. 67, № 6. – P. 661–663.

4. Бауместер Д. Физика квантовой информации / Д. Бауместер, А. Экерт, А. Цайлингер. – М.: Постмаркет, 2002. – 376 с.

5. 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.

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

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

8. 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.

9. 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.

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, № 3. – С. 372–379.

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

13. 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.

Statistical analysis of signals in quantum key distribution systems

In the paper we propose a model of amplification protocol with quantum key distribution by monitoring the levels of statistical error rate of key generation and distribution of quasi-one-photon states in quantum channel. The boundaries of the safety zone of a quantum channel for different types of attacks has been set.
Keywords: quantum key distribution system, secure key generation zone, PNS-attack.