УДК 621.383.523

А.С. Задорин, Д.А. Махорин

Интерферометрический контроль целостности данных в системе квантового распределения ключей с временным кодированием

Предложена схема повышения защищенности системы квантового распределения ключей по волоконно-оптическим линиям, основная на использовании двухпичковых проверочных кубитах, приготавливаемых и детектируемых интерферометрами Маха–Цендера.

Ключевые слова: квантовое распределение ключей, временное кодирование, интерференционный контроль проверочных кубитов.

Безусловная защищенность протоколов квантового распределения ключей (КРК) в открытых каналах связи гарантируется, как известно, общими физическими законами [1]. Однако эта гарантия в полной мере распространяется лишь на идеализированные, недиссипативные каналы. В реальных каналах с потерями защищенность систем КРК ограничивается некоторым предельно допустимым уровнем потерь $\xi_{кр}$, который связан с погонным затуханием света в квантовом канале, используемым протоколом и др. [2, 3]. Задача повышения $\xi_{кр}$, таким образом, оказывается одной из основных задач разработчиков, как протокола, так и программно-аппаратной части систем КРК. В большинстве случаев решение этой задачи основывается на расширении базовых протоколов дополнительными мерами контроля состояний последовательности кубитов $|\varphi_n\rangle$, которыми обмениваются удаленные легитимные пользователи А и Б (ПА и ПБ) системы КРК через квантовый канал [4–6]. К таким мерам относятся контроль статистики источника $|\varphi_n\rangle$ [5], статистики специально внедренных в общий поток $|\varphi_n\rangle$, состояний-ловушек (decoy states (DS)) [6], использование неортогональных состояний внутри базиса [7, 8] и др. В качестве базового при этом часто используется классический протокол BB84, адаптированный для передачи по одномодовому оптическому волокну (ОВ) последовательностей $|\varphi_n\rangle$ с фазовым (ФК) и временным (ВК) способами кодирования [9–15].

С точки зрения простоты реализации последний способ кодирования (BB84-ВК) представляется наиболее привлекательным. Однако его основным недостатком является сложность в обеспечении одного из фундаментальных системных требований – требования неортогональности временных квантовых состояний кубита $|\varphi\rangle$, обеспечивающего защиту квантового канала системы от атак условного агента E (AE).

Целью настоящей работы является обсуждение возможности усиления защищенности протокола BB84-ВК и увеличения битовой скорости B генерации ключевой последовательности (КП) за счет контроля когерентности состояний-ловушек – DS, специально приготавливаемых ПА в разбалансированном интерферометре Маха–Цендера (ИМЦ) [13–15].

Контроль состояний квантовых объектов при временном кодировании. Рассмотрим наиболее распространенный вариант протокола BB84-ВК, в котором последовательность кубитов $|\varphi_n\rangle$, представленных квазиоднофотонными состояниями (КОС) длительностью τ, приготавливается путем простого ослабления лазерного света. Здесь, как и в базовом протоколе BB84, пользователем А генерируется случайная последовательность $\mathbf{s}_А$, которая используется для кодирования последовательности КОС, т.е. формирования $|\varphi_n\rangle$. При этом пользователями А и Б независимо генерируются случайные последовательности $\mathbf{m}_А$, и $\mathbf{m}_Б$ переключения неортогональных базисов, на основе которых, после сверки по классическому каналу, на обеих сторонах канала формируются идентичные последовательности $\mathbf{m}_{АБ}$, пригодные для однозначной интерпретации принятых пользователем Б кубитов и формирования на этой основе ключевых последовательностей $\mathbf{k}_{АБ}$ [1, 4, 9].

Неортогональность квантовых состояний кубита $|\varphi\rangle$ в рассматриваемом случае обеспечивается несколькими способами [12, 14]. В первом из них данное условие обеспечивается за счет стробирования лазерного излучения электрооптическим модулятором (ЭОМ) и формирования коротких световых импульсов длительности Δ, сдвинутых во времени на величину $L \approx \Delta/2$ (рис. 1, *а*).

Трудность в реализации такого способа кодирования КОС связана со случайным пуассоновским распределением КОС внутри модулирующего сигнала электрооптического модулятора (ЭОМ). Это означает, что после необходимого ослабления светового импульса до уровня КОС его временное

положение будет флуктуировать внутри выделенного временного окна Δ. Данное обстоятельство не позволяет указанным способом обеспечить временное кодирование КОС на квантовом уровне, т.е. преобразовать эти квантовые объекты в кубиты.

Следует также учитывать, что на практике длительность τ отдельных элементов $|\varphi_n\rangle$, как правило, намного меньше длительности базисного окна Δ [10–15]. В этих условиях *AE* получает прямую возможность копирования кубитов, кодовое состояние $\mathbf{k}_{АБ}$ которых он позднее легко установит в результате прослушивания в классическом канале связи последовательности $\mathbf{m}_{АБ}$. Применение фазовых матриц (AWG) на входе ВОЛС [9] для выравнивания τ и Δ не может радикально устранить указанный риск взлома ключа.

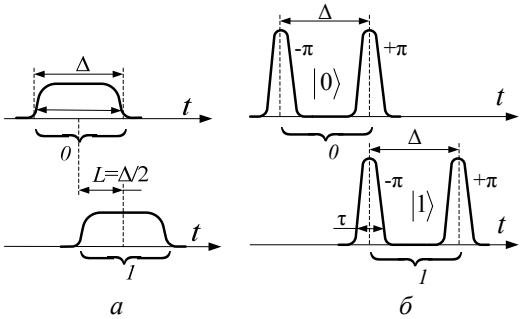

Рис. 1. Неортогональные кодовые состояния кубита в протоколе BB84-BK

В другом способе временного кодирования КОС, ассоциируемые с логической единицей, задерживаются во времени на величину δ относительно КОС с нулевым кодом. При этом кубиты $|0\rangle$ и $|1\rangle$ приготавливаются из указанных КОС за счет их дополнительного преобразования в интерферометре Маха–Цендера (ИМЦ), плечи которого разбалансированы по времени на величину Δ [12]. В результате такого преобразования кубиты $|0\rangle$ и $|1\rangle$ оказываются представленными суперпозицией из двух разделенных интервалом времени Δ динамических пичков, обозначенных на рис. 1, *б* символами ±π. Считается, что условие неортогональности здесь можно обеспечить за счет согласования задержки ИМЦ Δ с интервалом δ, при котором достигается совпадение второго и первого пичков кубитов $|0\rangle$ и $|1\rangle$ соответственно.

Как и в предыдущем случае, приготовленные указанным способом кубиты будут подвержены случайным временным флуктуациям. Однако временной интервал Δ между пичками в каждом из кубитов $|0\rangle$ и $|1\rangle$ при этом остается постоянным.

Следует подчеркнуть, что квантовые состояния кубитов $|\varphi_n\rangle$ в виде суперпозиция двух пичков ±π существует лишь до моментов их измерений. В ходе измерений двухпичковое состояние $|\varphi_n\rangle$ коллапсируют только в одно из двух возможных. Отсюда следует, что результаты измерений значения битрейта КОС на входе и выходе ИМЦ будут всегда одинаковы.

Важной особенностью квантовых объектов рассмотренного типа, образованных в результате суперпозиции нескольких КОС, является взаимная когерентность состояний ±π, степень которой может контролироваться, например, с помощью интерферометрических измерений. Отсюда следует, что попытка измерения или подмены любого из КОС названных квантовых объектов означает полное разрушение исходного кубита, следовательно, и когерентной связи между обоими пичками. Как уже отмечалось, этот факт может быть обнаружен посредством интерферометрического контроля (ИК), инструментальной основой которого может служить ИМЦ, аналогичный применявшемуся для приготовления кубитов.

Рассмотрим, например, возможность детектирования с помощью ИК UM-атаки (Unambiguous Measurements), т.е. атаки с измерениями с определенным исходом [7, 8] на протокол BB84-BK, построенный на основе двухпичковых кубитов. Как известно, для ее осуществления необходимо блокирование агентом *E* всех нечетких исходов. Из рис. 1, *б* видно, что в последовательности $|\varphi_n\rangle$ на выходе ИМЦ такие исходы представлены вторыми пичками в $|0\rangle$ и первыми в $|1\rangle$. Для детектирования указанных пичков, очевидно, необходимо провести последовательность измерений $|\varphi_n\rangle$, ведущих к коллапсу состояний $|\varphi_n\rangle$ и разрушению всех двухпичковых кубитов. Это означает 100% разрушение всей передаваемой по квантовому каналу последовательности $|\varphi_n\rangle$. Регистрация подобных нарушений целостности $|\varphi_n\rangle$ на стороне Б может осуществляться за счет интерферометрического контроля состояний кубитов $|\varphi_n\rangle$ в интерферометре Маха–Цендера. В рассматриваемом случае такая ИК обработка $|\varphi_n\rangle$ в ИМЦ позволяет установить когерентную связь между ±π для 50% кубитов исходной последовательности $|\varphi_n\rangle$ независимо от степени их поглощения в квантовом канале ξ.

Программно-аппаратную реализацию описанного выше метода ИК можно использовать в качестве дополнения к системе скалярного статистического контроля $|\varphi_n\rangle$ [16], усиливающего защищенность протокола BB84-BK.

Заметим далее, что организация ИК для всех элементов $|\varphi_n\rangle$, очевидно, усложняет аппаратуру системы, снижает скорость генерации ключа $\mathbf{k}_{АБ}$. Для преодоления названных проблем можно отка-

заться от тотального ИК, заменив его выборочным контролем целостности КОС в квантовом канале. С этой целью двухпичковые кубиты в основной последовательности $|\varphi_n\rangle$ удобно заменить на более простые – однопичковые КОС (см. рис. 1, *а*), без их обработки в ИМЦ. Контроль целостности потока $|\varphi_n\rangle$ в данном случае может осуществляться за счет случайного внедрения в указанную последовательность описанных выше двухпичковых DS-кубитов (DS-К), замаскированных под элементы $|\varphi_n\rangle$. Когерентность ±π-пичков в этих DS-К проверяется пользователем Б с помощью аналогичного ИМЦ после опубликования ПА в классическом канале сведений о номерах тактовых интервалах с внедренными в них DS-кубитами. Попытки в ходе PNS- или UM-атак подмены ±π-пичков в DS-К обычными КОС, как уже отмечалось, приводит к разрушению кубитов и потере когерентности между указанными состояниями, которая и обнаруживается ПА с помощью ИК в ИМЦ. Программно-аппаратная реализация описанного алгоритма представлена на структурной схеме рис. 2.

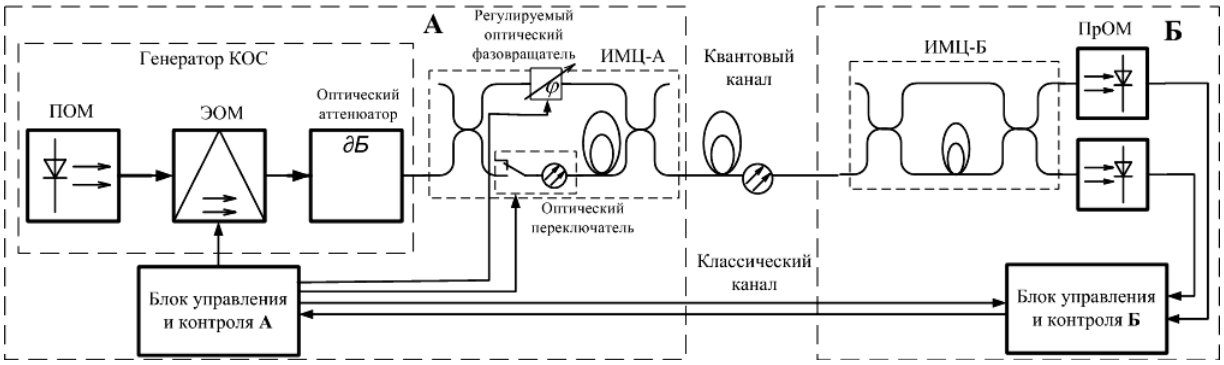

Рис. 2. Структурная схема КРК-ВК с интерферометрическим контролем квантовых состояний DS-К

Здесь формируемый на стороне ПА поток КОС $|\varphi_n\rangle$ через одно из плеч ИМЦ-А передается в квантовый канал. Второе плечо интерферометра используется для приготовления проверочных двухпичковых DS-кубитов в моменты коммутации оптического переключателя в ИМЦ-А. В приемнике КОС обрабатываются в ИМЦ-Б, аналогичном ИМЦ-А. Каждое из этих устройств имеет четыре оптических порта, объединенных между собой системой зеркал и светоделителей. В системе из сбалансированных ИМЦ связь входных $|\varphi_i\rangle$ и выходных $|\varphi_0\rangle$ КОС интерферометров обеспечивается сверткой матричных операторов **H** и **P**, описывающих светоделительные и фазосдвигающее устройства в их плечах [9]:

$$|\varphi_o\rangle = \mathbf{H}\cdot\mathbf{P}\cdot\mathbf{H}\cdot|\varphi_i\rangle. \tag{1}$$

Здесь

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathbf{P} = \begin{bmatrix} e^{j\varphi_0} & 0 \\ 0 & e^{j\varphi_1} \end{bmatrix},$$

φ_0, φ_1 – фазовые сдвиги в плечах интерферометра, задаваемые регулируемым оптическим фазовращателем (см. рис. 2).

Из приведенных формул следует, что при возбуждении КОС входного порта первого интерферометра вероятности P_3 и P_4 попадания этих квантовых объектов в соответствующие выходные порты ИМЦ определяют видность интерференционной картины, образованной ±π-пичками DS-К:

$$P_3 = \cos^2\left(\frac{\Delta\varphi}{2}\right), \quad P_4 = \sin^2\left(\frac{\Delta\varphi}{2}\right), \tag{2}$$

где $\Delta\varphi = \varphi_0 - \varphi_1$.

Выходные сигналы приемных оптических модулей (ПрОМ), пропорциональные P_3 и P_4, таким образом, могут использоваться для контроля целостности случайной последовательности DS-кубитов.

Подобная структура ИК-защиты системы КРК рассматривалась ранее в работах [14, 15]. В схеме этих авторов предлагалось использовать поток КОС вида рис. 1, *а*. При этом в приемнике ПБ $|\varphi_i\rangle$ разделяется на две равные части. Одна из них регистрировалась ПрОМ-2 и использовалась для ИК, а другая, с выхода ПрОМ-1, – для формирования последовательностей $\mathbf{k}_{АБ}$. Указанное прореживание потока КОС за счет отвода половины в канал контроля когерентности, очевидно, снижает скорость генерации ключа системой, пропорциональной коэффициенту деления оптического сплитера на стороне ПБ.

Заключение. Предложенная выше схема оптоволоконной КРК-BB84-BK, основанная на использовании двухпичковых проверочных кубитов, свободна от указанного недостатка и позволяет повысить уровень защищенности генерации ключа.

Литература

1. Bennett C.H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. – 1992. – Vol. 68. – P. 3121.

2. Brassard G. Limitations on practical quantum cryptography / G. Brassard, N. Lütkenhaus, T. Mor, B.C Sanders // Phys. Rev. Lett. – 2000. – Vol. 85. – P. 1330–1333.

3. 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.

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

5. 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.

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

7. Scarani V. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations / V. Scarani, A. Acin, G. Ribordy, N. Gisin // Phys. Rev. Lett. – 2004. – Vol. 92. – P. 057901.

8. Кронберг Д.А. Квантовое распределение ключей в однофотонном режиме с неортогональными состояниями внутри базиса / Д.А. Кронберг, С.Н. Молотков // Письма в ЖЭТФ. – 2009. – Т. 89, вып. 7. – С. 432–438.

9. Имре Ш. Квантовые вычисления и связь. Инженерный подход / Ш. Имре, Ф. Балаж. – М.: Физматлит, 2008. – 320 с.

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

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

12. Молотков С.Н. Мультиплексная квантовая криптография с временным кодированием без интерферометров // Письма в ЖЭТФ. – 2004. – Т. 79, вып. 9. – С. 554–559.

13. Debuisschert T. Time coding protocols for quantum key distribution / T. Debuisschert, W. Boucher // Phys. Rev. A. – 2004. – Vol. 70, Iss. 4. – P. 042306.

14. 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.

15. Хорошко Д.Б. Квантовое распределение ключа на временных сдвигах: чувствительность к потерям / Д.Б. Хорошко, Д.И. Пустоход, С.Я. Килин // Оптика и спектроскопия. – 2011. – Т. 111, вып. 5. – С. 719–723.

16. Задорин А.С. Статистическая обработка сигналов в системах квантового распределения ключа / А.С. Задорин, Д.А. Махорин // Доклады ТУСУРа. – 2014. – №3 (33). – С. 90–93.

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 ТУСУРа
Тел.: 8-913-824-11-11
Эл. почта: mda.tomsk@gmail.com

Zadorin A.S., Makhorin D.A.

Interferometric control of data integrity in the system of quantum key distribution based on time coding

A scheme to improve the security of quantum key distribution over fiber-optic lines, mainly in the use of check qubits which are prepared and detected Mach-Zehnder interferometer has been proposed.
Keywords: quantum key distribution, time coding, interference control verification qubits.