НАНОСИСТЕМЫ: ФИЗИКА, ХИМИЯ, МАТЕМАТИКА, 2012, 3 (3), С. 92–98

УДК 004.27:530.145

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ ПОЛЯРИЗАЦИОННЫХ ИСКАЖЕНИЙ СИГНАЛА В СИСТЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ

С. М. Кынев, А. Е. Иванова, В. И. Егоров, А. В. Глейм, А. В. Рупасов, С. А. Чивилихин

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

egorovvl@gmail.com, aglejm@yandex.ru

PACS 03.67.-a

Рассмотрена аналитическая модель, описывающая поляризационные искажения оптического сигнала при его прохождении по волоконной линии связи. Модель применена для описания принципов компенсации искажений слабого сигнала в различных типах систем квантовой криптографии.

Ключевые слова: квантовая криптография, двулучепреломление, зеркала Фарадея.

1. Введение

Практической реализации систем квантовой криптографии [1–4] препятствует ряд технических проблем, вызванных существенным отличием реальных оптических устройств от их идеализированного представления. Одной из них является негативное воздействие двулучепреломления в оптическом волокне и других элементах линии связи, искажающее поляризацию квантового сигнала и отрицательно сказывающееся на операционной скорости, эффективности, безопасности и надёжности систем квантовой криптографии.

В устройствах, использующих поляризационное кодирование [1], необходимо сохранять этот параметр сигнала на всей протяжённости оптического тракта. В этом случае единственной возможностью, по-видимому, является использование дорогостоящих специальных оптических волокон, сохраняющих поляризацию. В установках, в которых в качестве модулируемого параметра выступает фаза излучения [2], достаточно обеспечивать только одинаковость поляризации интерферирующих фотонов в момент их взаимодействия, что значительно снижает требования к сохранению поляризации. Переход к согласованным plug-and-play системам позволяет решить эту задачу с помощью зеркал Фарадея [3]. В системах квантовой рассылки ключа на поднесущих частотах модулированного излучения (КРКПЧ) [4] отсутствует необходимость пассивного контроля поляризации, так как изменение характеристик центральной и боковых (поднесущих) частот при прохождении по оптическому волокну остаётся одинаковым. В этих системах, однако, требует решения проблема компенсации поляризационной зависимости электрооптических модуляторов.

Несмотря на то, что на практике указанные проблемы были успешно решены, на сегодняшний день отсутствует устоявшийся способ теоретического представления поляризационных искажений. Это связано с тем, что точное аналитическое описание двулучепреломления в волокне является затруднительным. Отдельные участки линии связи имеют различные характеристики и испытывают разные внешние воздействия; поэтому направление быстрой и медленной осей в них изменяется во времени и пространстве случайным образом [5]. В работе [6] была предложена операторная модель двулучепреломления и поляризационной модовой дисперсии, хорошо подходящая для описания систем квантовой

информатики. В данной работе модель применена к системам квантовой криптографии: продемонстрирована эволюция сигнала в линиях оптической связи и рассмотрены известные механизмы компенсации искажений.

2. Поляризационные искажения сигнала в системах квантовой криптографии

В любой точке линии связи импульс поляризованного излучения можно разделить на две ортогональные поляризационные моды. В идеальном волокне с цилиндрической сердцевиной при отсутствии дефектов эти составляющие не претерпевали бы изменений, и состояние поляризации сохранялось бы. Однако реальное волокно характеризуется различием формы сердцевины по длине тракта из-за механических и тепловых воздействий при эксплуатации, дефектов в местах соединений и разветвлений, а также неравномерностей, образующихся в процессе производства. Все эти факторы приводят к возникновению двулучепреломления и поляризационной модовой дисперсии, и импульс, распространяясь в волокне, постепенно приобретает произвольную поляризацию [5].

Вклад других элементов является постоянной величиной, определяемой их физическими характеристиками. В частности, в электрооптических модуляторах используются нелинейные кристаллы, обладающие сильным двулучепреломлением. При прохождении света через них происходит побочное изменение поляризации, так как одна из поляризационных мод задерживается относительно другой. Кроме того, ортогональные моды при прохождении через модулятор претерпевают различные фазовые сдвиги. Это приводит к тому, что синфазные, но по-разному поляризованные, волны после прохождения одного и того же модулятора имеют разную фазу.

В квантовой криптографии, при работе с предельно слабыми сигналами, на передний план выходит ослабление интерференционных эффектов, вызванное искажениями поляризации импульсов. Ортогонально поляризованные когерентные монохроматические волны не интерферируют; при сложении интенсивность результирующей волны равна сумме интенсивностей двух волн, а поляризация изменяется в соответствии с разностью фаз между компонентами. Максимальная пиковая интенсивность интерференционной картины достигается для одинаково поляризованных синфазных волн (рис. 1). Следует учитывать, что невозможным оказывается применение усилителей и компенсаторов. Таким образом, контроль разности фаз и поляризации фотонов в системах квантовой криптографии является обязательным, так как его отсутствие накладывает серьёзные ограничения на скорость генерации ключа и дальность передачи.

3. Математическое описание поляризационных искажений

Предложенный в работе [6] метод описания поляризационных искажений в волокне заключается в следующем. Оптическое волокно можно разделить на несколько участков небольшого размера, предположив, что в каждом из них волокно имеет различные направления «быстрой» и «медленной» осей двулучепреломления (рис. 2).

Выбранные направления по всей протяженности волокна считаются независимыми от времени: это упрощение допустимо в системах квантовой криптографии, где длительность прохождения сигнала на несколько порядков меньше характерного времени флуктуации двулучепреломления [5]. В этом случае двулучепреломление и поляризационно-модовую дисперсию можно описать операторами в матричной форме. Пусть состояние поляризации на n-ом участке задано вектором поляризационных мод:

$$E_n = \begin{pmatrix} E_{x_n} \\ E_{y_n} \end{pmatrix}. \tag{1}$$

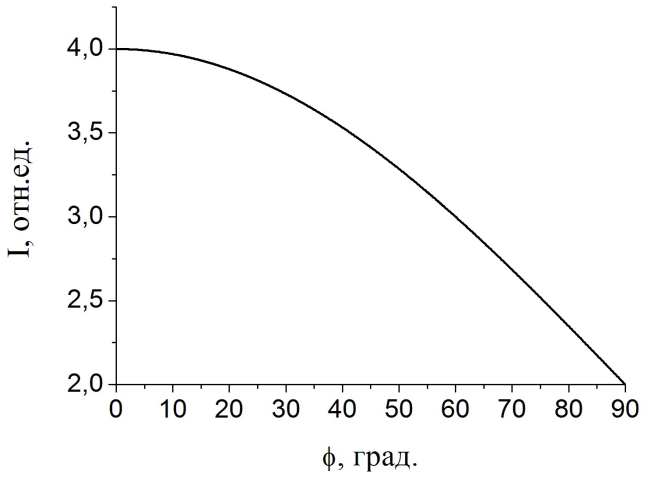

РИС. 1. Зависимость пиковой интенсивности от угла между плоскостями поляризации интерферирующих импульсов

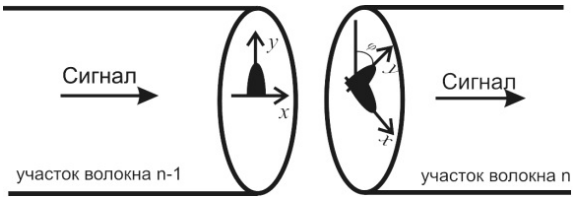

РИС. 2. Изменение ориентации «быстрой» и «медленной» осей на соседних участках волокна

Обмен энергией между модами характеризуется матрицей вращения, угол φ задает изменение ориентации быстрой и медленной осей на каждом участке:

$$R_{n-1} = \begin{pmatrix} \cos\phi_{n-1} & \sin\phi_{n-1} \\ -\sin\phi_{n-1} & \cos\phi_{n-1} \end{pmatrix}, \tag{2}$$

а поляризационно-модовая дисперсия задана матрицей фазовой задержки:

$$L_n = \begin{pmatrix} e^{-i\omega\left(T_n+\frac{\delta\tau_n}{2}\right)} & 0 \\ 0 & e^{-i\omega\left(T_n-\frac{\delta\tau_n}{2}\right)} \end{pmatrix}, \tag{3}$$

где T_n — средняя групповая задержка, а $\delta\tau n$ характеризует поляризационно-модовую дисперсию на n-ном интервале, связанную с двулучепреломлением соотношением:

$$\delta\tau = \frac{Bz}{c}, \tag{4}$$

где B — разница показателей преломления для ортогональных мод, z — длина участка волокна, c — скорость света в вакууме. Тогда изменение поляризации импульса при проходе по оптическому тракту можно представить как действие операторов L и R на вектор E:

$$E_n = L_n \cdot R_{n-1} \cdot E_{n-1}. \tag{5}$$

Сопоставив каждому участку волокна матрицу со случайными параметрами, а каждому оптическому элементу – с предварительно заданными, смоделируем преобразования импульса при прохождении света по линии связи. Рассмотрим, какое влияние оказывает двулучепреломление классической схеме протокола B92 (рис. 3).

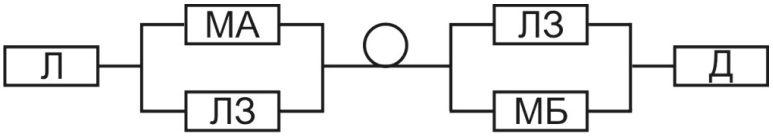

РИС. 3. Схема простейшей реализации протокола B92: Л — Лазер; МА — модулятор Алисы; МБ — модулятор Боба; ЛЗ — линии задержки; Д — детектор фотонов

Выражения (6) и (7) описывают изменение поляризация импульсов, прошедших по разным плечам интерферометра. Порядок прохождения первого импульса: задержка Алисы (R_{DA}), линия связи (R_F), модулятор Боба (R_{MB}); порядок прохождения второго импульса — модулятор Алисы (R_{MA}), линия связи, задержка Боба (R_{DB}).

$$E_1 = R_{DA} \cdot R_F \cdot R_{MB} \cdot E_n, \tag{6}$$

$$E_2 = R_{MA} \cdot R_F \cdot R_{DB} \cdot E_n. \tag{7}$$

Так как в общем случае $R_{DA} \neq R_{DB}$, $R_{MA} \neq R_{MB}$, состояния поляризации в такой системе не только не сохраняются, но и подвергаются неодинаковым искажениям, так как импульсы проходят различные пути. Это приводит к снижению видности интерференционной картины, тем самым уменьшая скорость генерации и увеличивая коэффициент ошибок.

4. Моделирование компенсации искажений в системах Plug&Play

Как было указано выше, одним из возможных решений проблемы сохранения поляризации является создание согласованных систем (рис. 4).

В plug-and-play системах поляризационные искажения компенсируются за счёт обратного прохода импульсов по оптическому тракту после отражения от фарадеевского зеркала, меняющего местами поляризационные компоненты импульса (как отмечено выше, R считается независимым от времени). Простейшее зеркало Фарадея представляет собой

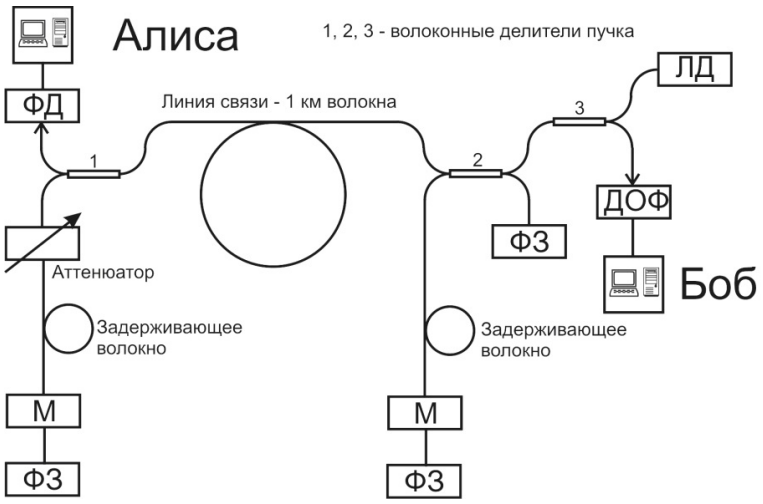

РИС. 4. Схема Plug-and-play системы квантовой криптографии (ЛД — лазерный диод; ФЗ — зеркала Фарадея; М — фазовый модулятор; ДОФ — детектор одиночных фотонов; ФД — фотодетектор; 1, 2, 3 — делители пучка)

комбинацию из 45-градусного фарадеевского вращателя и зеркала. В двухпроходной оптической схеме, состоящей из такого зеркала и установленного перед ним взаимного элемента с произвольной фазовой анизотропией (например, отрезка одномодового оптического волокна), выходная поляризация всегда ортогональна входной, независимо от анизотропии и входной поляризации [7]. Это позволяет стабилизировать поляризацию на выходе двухпроходной анизотропной оптической системы с нестабильными параметрами.

Представим действие фарадеевского зеркала оператором T:

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{8}$$

Тогда перед детектированием состояния поляризации интерферирующих фотонов описываются выражениями:

$$E_1 = R_{MB} \cdot T \cdot R_{MB} \cdot R_{DB} \cdot T \cdot R_{DB} \cdot R_F \cdot R_{DA} \cdot R_{MA} \cdot T \cdot R_{MA} \cdot R_{DA} \cdot R_F \cdot E_0 = E_0, \tag{9}$$

$$E_2 = R_F \cdot R_{DA} \cdot R_{MA} \cdot T \cdot R_{MA} \cdot R_{DA} \cdot R_F \cdot R_{DB} \cdot T \cdot R_{DB} \cdot R_{MB} \cdot T \cdot R_{MB} \cdot E_0 = E_0, \tag{10}$$

то есть сохраняются. Это достигается ценой уменьшения скорости передачи и возрастания потерь, так как сигнал проходит удвоенное расстояние по линии связи.

Если заменить в схеме зеркала Фарадея обычными (что в математическом представлении эквивалентно замене оператора T единичной матрицей), то состояния поляризации не сохранятся, хоть и претерпевают одинаковое искажение. Это происходит благодаря тому, что в plug-and-play системах пучки проходят одинаковый путь. Несмотря на то, что в этом случае видность интерференционной картины будет значительно выше, чем в ситуации с разными поляризациями, зеркала Фарадея, как будет показано ниже, нужно использовать для компенсации поляризационной зависимости модуляторов Алисы и Боба, а также поскольку линейно поляризованные импульсы обладают наивысшим контрастом интерференционной картины.

5. Моделирование компенсации искажений в системах КРКПЧ

В системах КРКПЧ (рис. 5) необходимость контроля поляризации в волокне отсутствует.

Действительно, так как слабый сигнал на поднесущих частотах распространяется вместе с высокоинтенсивной несущей, на всём протяжении оптической линии связи компоненты импульса испытывают одинаковые изменения поляризации. В результате, после модуляции на приёмном узле видность интерференционной картины будет высокой. Тем не менее, это не снимает проблемы, связанной с поляризационной зависимостью фазовых модуляторов. Покажем, что использование зеркала Фарадея позволяет компенсировать

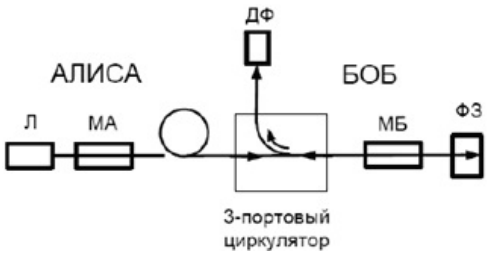

РИС. 5. Принципиальная схема системы квантовой рассылки ключа на поднесущих частотах (Л — лазер; МА, МБ — модуляторы; ФЗ — зеркало Фарадея)

негативные эффекты поляризационно-модовой дисперсии. Для этого возьмем импульс с произвольным значением поляризации (1) и применим к нему оператор фазовой задержки (3), что продемонстрирует первое прохождение импульса через фазовый модулятор:

$$L_n \cdot \begin{pmatrix} E_x \\ E_y \end{pmatrix} = \begin{pmatrix} E_x e^{-i\omega\left(T_n + \frac{\tau_n}{2}\right)} \\ E_y e^{-i\omega\left(T_n - \frac{\tau_n}{2}\right)} \end{pmatrix}. \tag{11}$$

После отражения от зеркала Фарадея компоненты импульса поменяются местами:

$$T \cdot L_n \cdot \begin{pmatrix} E_x \\ E_y \end{pmatrix} = \begin{pmatrix} E_y e^{-i\omega\left(T_n - \frac{\tau_n}{2}\right)} \\ E_x e^{-i\omega\left(T_n + \frac{\tau_n}{2}\right)} \end{pmatrix}. \tag{12}$$

После второго прохождения через модулятор получаем:

$$L_n T \cdot L_n \cdot \begin{pmatrix} E_x \\ E_y \end{pmatrix} = \begin{pmatrix} E_y e^{-i\omega(2T_n)} \\ E_x e^{-i\omega(2T_n)} \end{pmatrix}. \tag{13}$$

Видно, что эффекты двулучепреломления компенсировались (в показателе экспоненты отсутствует зависимость от τ_n), а фаза излучения при выключенном модуляторе определяется только временем прохождения света через устройство.

6. Заключение

Таким образом, аналитическая модель двулучепреломления в волокне с использованием матриц вращения и фазовой задержки была эффективно применена для описания искажений слабого сигнала в системах квантовой рассылки ключа нескольких типов и механизмов компенсации поляризационных искажений в них. Было показано, что практическая рассылка секретного ключа возможна лишь в двухпроходовых (plug-and-play) или однопроходовых (КРКПЧ) схемах, имеющих встроенный механизм компенсации искажений слабого сигнала. В обоих случаях зеркала Фарадея могут быть эффективно применены как для компенсации эффектов двулучепреломления и поляризационной модовой дисперсии, так и поляризационной зависимости фазовых модуляторов. Лежащий в основе теоретического описания операторный подход является традиционным в квантовой информатике, что значительно расширяет границы его применимости. В частности, он может быть использован для иллюстрации преобразований поляризации фотонов в оптических схемах, реализующих элементы квантового компьютера.

Работа выполнена в рамках тематического плана научно-исследовательских работ НИУ ИТМО.

Литература

[1] Bennett C., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. — 1984. — P. 175-179.

[2] Bennett C.H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. — 1992. — V. 68. — P. 3121-3124.

[3] Muller A., Herzog T., Huttner B., Tittel W., Zbinden H., Gisin N. «Plug and play» systems for quantum cryptography // Appl. Phys. Lett. — 1997. — V. 70. — P. 793-795.

[4] Мазуренко Ю.Т., Мероллa Ж.-М., Годжебюр Ж.-П. Квантовая передача информации с помощью поднесущей частоты. Применение к квантовой криптографии // Оптика и спектроскопия. — 1999. — Т. 86. — № 2. — С. 181-183.

[5] Agrawal G.P. Fiber-optic communication systems. — John Wiley & Sons Publications, NY. — 2002. — 548 p.

[6] Suetsugu Y., Kato T., Kakui M., Nishimura M. Effects of random mode coupling on polarization mode dispersion and power penalty in single-mode fiber systems // Optical Fiber Technology. — 1994. — V. 1. — P. 81-86.

[7] Геликонов В.М., Геликонов Г.В., Иванов В.В., Новиков М.А. Фарадеевский компенсатор взаимной оптической анизотропии на основе поляризационного кольцевого интерферометра // Письма в ЖТФ. — 1999. — Т. 25. — № 10. — С. 57-63.