УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА
Том 155, кн. 1 Физико-математические науки *2013*

УДК 535.14

КОМПЕНСАЦИЯ ОШИБОК ПРИ РАСПРЕДЕЛЕНИИ КВАНТОВОГО КЛЮЧА С ПОМОЩЬЮ ПЕРЕПУТАННЫХ ПОЛЯРИЗАЦИОННЫХ СОСТОЯНИЙ БИФОТОНОВ

Г.П. Мирошниченко, А.А. Сотникова

Аннотация

Рассмотрены оптимальные стратегии выбора отрезков оптического волокна для квантовых каналов Алисы и Боба, которые используются для распределения квантового ключа с помощью перепутанных поляризационных состояний бифотонов. В работе показано, что среднее относительное число ошибок в просеянном ключе можно существенно уменьшить, даже при больших дисперсиях случайных параметров оптического волокна. Для этого каналы Алисы и Боба следует проектировать из волокна, изготовленного по идентичной технологии. Выбор пар отрезков оптического волокна следует производить коррелированно, с коэффициентом корреляции, близким к 1.

Ключевые слова: квантовая криптография, ЭПР-протокол, среднее относительное число ошибок, оптическое волокно.

Введение

В настоящее время разработаны одномодовые оптические волокна (ОВ) с малым поглощением (в окнах прозрачности), которые находят широкое применение в оптических коммуникационных системах на дальние расстояния с высокой скоростью передачи битов информации. Различные воздействия на ОВ приводят к появлению взаимодействия между ортогонально поляризованными модами, вызывая в ОВ эффект двулучепреломления или оптической активности [1–4]. Особенности искажения классической информации в одномодовом ОВ подробно изучены. Оптическая активность возникает при скручивании ОВ, эффект двулучепреломления связан с кривизной, натяжением, деформацией ОВ. В работах [2, 3] изложена теория связанных мод, описывающая взаимодействие двух ортогонально поляризованных мод в одномодовом ОВ в присутствии эффектов изгиба, кручения, деформации. В этих работах развита теория поляризационной модовой дисперсии, то есть зависимости групповой скорости волны в ОВ от состояния ее поляризации. В работах [2–4] предложена теория поляризационной модовой дисперсии, то есть зависимости групповой скорости волны в ОВ от состояния ее поляризации. В этих же работах дана теория эволюции поляризации классической волны с учетом поляризационной модовой дисперсии и случайного характера ОВ, где в качестве стохастического процесса, описывающего случайную зависимость параметров ОВ от расстояния, выбран винеровский процесс. Как следствие, в [2–4] удалось объяснить зависимость параметра поляризационной модовой дисперсии от корня квадратного длины ОВ.

Новым направлением современной информатики являются оптические квантовые информационные технологии. С использованием принципов квантовой оптики действуют протоколы квантовых коммуникаций – квантовая криптография,

квантовая телепортация, плотное кодирование. Здесь по ОВ передается квантовая информация, то есть информация, закодированная на квантовых состояниях фотонов – кубитах. Кубиты можно создавать на квантовых состояниях поляризации фотонов. В настоящее время существуют несколько практических схем квантовой криптографии. В работе [6] использовано кодирование информации на поляризационных степенях свободы фотонов, практическая реализация квантовой криптографии по ЭПР-протоколу с использованием перепутанных поляризационных состояний бифотонов предложена в работе [5]. В идеале, в установке квантовой криптографии должны использоваться однофотонные состояния оптической моды. Просеянный ключ после этапа согласования базисов подвергается классическим схемам исправления ошибок и повышения секретности, после чего получают криптографический ключ. Есть много причин, по которым просеянный ключ содержит ошибки. В литературе степень секретности характеризуют синтетическим параметром – скоростью появления ошибок в квантовых битах, которая зависит от различных физических свойств квантового канала, передатчика, приемника, стратегии перехвата и других характеристик, в частности от относительной ошибки в квантовом ключе, оставшейся после этапа просеивания. В настоящей работе аналитически изучается зависимость суммарной относительной ошибки в генерации просеянного ключа с помощью перепутанных поляризационных состояний бифотонов. Рассмотрены оптимальные стратегии выбора отрезков ОВ для квантовых каналов Алисы и Боба. В работе показано, что среднее относительное число ошибок в просеянном ключе можно существенно уменьшить, если выбор пар отрезков ОВ производить коррелированно с коэффициентом корреляции, близким к 1.

1. Влияние случайного ОВ на квантовые поляризационные состояния фотонов

Состояние классической поляризации излучения принято описывать точкой на сфере Пуанкаре, координаты данной точки называются параметрами Стокса волны. В квантовой оптике параметры Стокса фотонов имеют смысл тройки некоммутирующих операторов, подчиняющихся коммутационным соотношениям алгебры su(2): $\widehat{S}_x$, $\widehat{S}_y$, $\widehat{S}_z$. Здесь x, y, z – система координат с центром в центре сферы Пуанкаре. В квантовой оптике (в отличие от классической) не существует состояний, где три оператора $\widehat{S}_x$, $\widehat{S}_y$, $\widehat{S}_z$ имели бы точные (без дисперсии) значения. Но можно ввести собственные состояния оператора $\widehat{S}_z$ и оператора Казимира $\widehat{S}^2$ и в базисе этих состояний описывать развитие состояний фотонов при их распространении по ОВ. Опишем состояние фотонов, распространяющихся по одномодовому ОВ. Обозначим через $|V\rangle$ ($|H\rangle$) состояние одного вертикально (горизонтально) поляризованного фотона в ОВ. В подпространстве одного фотона в моде операторы Стокса имеют вид матриц Паули $S_x = \sigma_x$, $S_y = \sigma_y$, $S_z = \sigma_z$, $\widehat{S}^2 = \widehat{I}$. Базис $|V\rangle$, ($|H\rangle$) является собственным для матрицы S_z ($\widehat{S}^2$): $S_z|H\rangle = |H\rangle$ ($S_z|V\rangle = -|V\rangle$). Квантовое состояние фотонов изменяется в процессе распространения по ОВ. В шредингеровском представлении необходимо определить зависящую от времени матрицу плотности фотонов в ОВ

$$\rho(t) = \frac{1}{2}\left(I + \left(\mathbf{p}(t), \widehat{\mathbf{S}}\right)\right). \tag{1}$$

Здесь $\mathbf{p}(t)$ – средний вектор Стокса фотона, $\widehat{\mathbf{S}}$ – операторный вектор с компонентами $\widehat{S}_x$, $\widehat{S}_y$, $\widehat{S}_z$. Развитие во времени матрицы $\rho(t)$ определяется оператором развития, который при феноменологическом подходе параметризуется несколькими

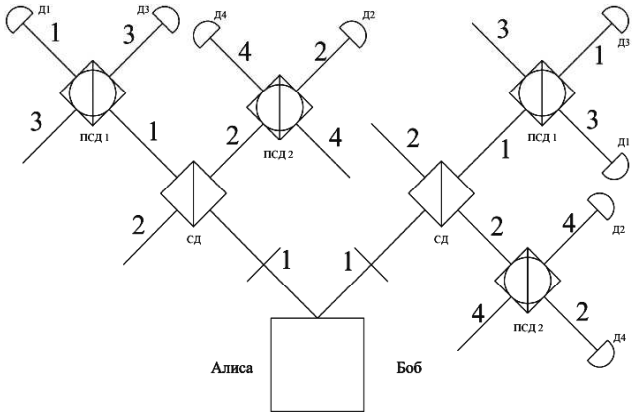

Рис. 1. ПСД1, ПСД2 – поляризационные светоделители с наклонным и вертикально-горизонтальным базисом соответственно, СД – светоделитель, Д1, Д2, Д3, Д4 – детекторы фотонов

параметрами, величины которых определяются технологией изготовления ОВ

$$\rho\left(t\right)=U\left(t,\boldsymbol{\xi}\right)\rho\left(0\right)U\left(t,\boldsymbol{\xi}\right)^{\clubsuit},\quad U\left(t,\boldsymbol{\xi}\right)=\exp\left(-iHt\right). \tag{2}$$

Здесь $H=\left(\boldsymbol{\xi},\widehat{\mathbf{S}}\right)/2$ – феноменологический гамильтониан фотонов в ОВ (в резонансном представлении), $\boldsymbol{\xi}$ – случайный вектор параметров ОВ. В рассматриваемом подходе пренебрегается деполяризацией и поглощением фотонов. Введем сферические координаты вектора параметров

$$\boldsymbol{\xi}=\xi\boldsymbol{\epsilon},\quad \epsilon_z=\cos\theta,\quad \epsilon_x=\sin\theta\cos\phi,\quad \epsilon_y=\sin\theta\sin\phi. \tag{3}$$

Рассмотрим два физически различимых случая. Первый случай ($\theta=\pi/2$, $\phi=c\pi/2$) – фарадеевское вращение, которое описывается случайным поворотом среднего вектора Стокса $\mathbf{p}(t)$ на угол $\omega=\xi t$ вокруг оси y. Второй случай ($\phi=0$) – случайное двулучепреломление в ОВ с ориентацией оси «кристалла» под углом $\theta/2$ в плоскости поляризации по отношению к горизонтальной оси и разностью фаз между «быстрым» и «медленным» направлением $\omega=\xi t$. Двулучепреломление описывается случайным поворотом среднего вектора Стокса $\mathbf{p}(t)$ на угол $\omega=\xi t$ вокруг оси, лежащей в плоскости xz под углом θ к оси z.

2. Схема распределения квантового ключа с помощью перепутанных поляризационных состояний бифотонов

Установка квантовой криптографии, схема которой представлена на рис. 1, состоит из генератора перепутанных по поляризационным состояниям фотонов и двух анализаторов на передающей станции (Алиса) и приемной (Боб), соединенных с ЭПР-генератором отрезками ОВ – квантовыми каналами. ЭПР-генератор является источником синглетных состояний бифотонов

$$\left|\Psi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|H\right\rangle_A\left|V\right\rangle_B-\left|V\right\rangle_A\left|H\right\rangle_B\right).$$

Здесь символами A и B отмечены фотоны в каналах Алисы и Боба. Генерация ключа осуществляется по BB84-протоколу, состоящему из четырех состояний поляризации фотона в канале Алисы и в канале Боба. На каждый посланный в ЭПР-канал бифотон (в случае идеальных детекторов и в отсутствие потерь фотонов)

откликается один из четырех детекторов Алисы и один из четырех детекторов Боба. Всего анализаторы Алисы и Боба фиксируют 16 парных событий – совпадений щелчков детекторов Алисы и Боба. На этапе просеивания ключа половина событий отбрасывается при согласовании базисов по открытому каналу. Согласно рис. 1 отбрасываются в процессе просеивания события, когда одновременно срабатывают детекторы с номерами противоположной четности

$$D_1^A \wedge D_2^B, \quad D_1^A \wedge D_4^B, \quad D_2^A \wedge D_1^B, \quad D_2^A \wedge D_3^B,$$
$$D_3^A \wedge D_2^B, \quad D_3^A \wedge D_4^B, \quad D_4^A \wedge D_1^B, \quad D_4^A \wedge D_3^B.$$

Остальные 8 событий формируют квантовый код. Алиса присваивает значение "0" квантовых битов, если сработали детекторы D_1^A или D_2^A, и значение "1", если сработали детекторы D_3^A или D_4^A. Аналогичные значения битам присваивает Боб. Но из-за ошибок в квантовом канале возможны несовпадающие по номерам отсчеты у Алисы и Боба. Это

$$D_1^A \wedge D_3^B, \quad D_3^A \wedge D_1^B, \quad D_2^A \wedge D_4^B, \quad D_4^A \wedge D_2^B.$$

Предположим, что причина появления ошибки в коде Боба связана со случайным изменением состояния поляризации фотонов Алисы и Боба при распространении бифотона от генератора к анализаторам (анализаторы считаются идеальными). Матрицы плотности фотонов на входе анализаторов будут определяться выражениями (1)–(3), определяемыми случайными векторами в канале Алисы и Боба – $\boldsymbol{\xi}_A$, $\boldsymbol{\xi}_B$. В настоящей работе будем предполагать, что эти параметры случайны в ансамбле отрезков ОВ, изготовленных по одной технологии, которая характеризуется определенным разбросом параметров $\boldsymbol{\xi}$. Приведем формулу для вероятности ошибки при передаче одного кубита по ОВ со случайным двулучепреломлением (BF) при фиксированных значениях случайных углов векторов $\boldsymbol{\xi}_A$, $\boldsymbol{\xi}_B$:

$$P_{\text{err}}^{\text{BF}} = \frac{1}{4}\left(1 - \frac{1}{2}\left((1-\cos\omega_A)(1-\cos\omega_B)\cos(\theta_B-\theta_A)^2 + \right.\right.$$
$$\left.\left. + \sin\omega_A\cos(\theta_B-\theta_A)\sin\omega_B + \cos\omega_B + \cos\omega_A\right)\right). \quad (4)$$

Формула для вероятности ошибки в переданном кубите по ОВ со случайным эффектом Фарадея (F) имеет вид

$$P_{\text{err}}^{\text{F}} = \frac{1-\cos(\omega_A-\omega_B)}{4}. \quad (5)$$

Здесь символами A, B отмечены случайные параметры (3) $\omega_A = \xi_A t$, $\omega_B = \xi_B t$, θ_A, θ_B в канале Алисы и Боба. При проектировании квантового канала на ОВ естественно ориентироваться на средние характеристики ОВ выбранного типа. Среднюю вероятность ошибки получим, усреднив $P_{\text{err}}^{\text{BF}}$ или $P_{\text{err}}^{\text{F}}$ по разбросу параметров ω_A, ω_B, θ_A, θ_B.

Рассмотрим два случая. В первом случае предположим, что выбор пары оптических волноводов в каналах (Алисы и Боба) производится коррелированно, плотность вероятности коррелированных пар x, y будем вычислять по формуле нормального распределения, где r – коэффициент корреляции (математическое ожидание полагается равным нулю), дисперсии случайных переменных в паре положим равными σ^2

$$W(\sigma, r, x, y) = \frac{1}{2\pi\sigma^2\sqrt{1-r^2}}\exp\left(-\frac{x^2+y^2-2rxy}{2\sigma^2(1-r^2)}\right).$$

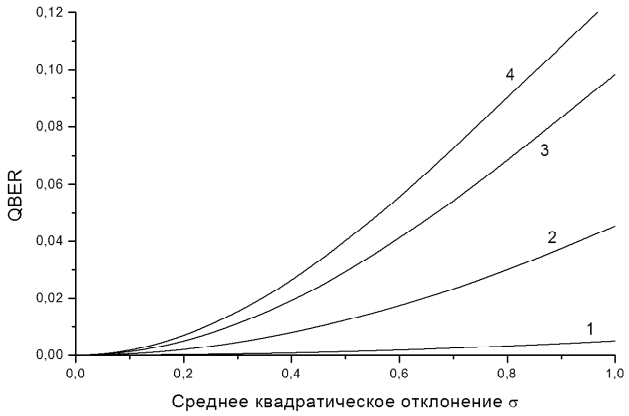

Рис. 2. Зависимость средней относительной ошибки в просеянном квантовом ключе QBER для случайного двулучепреломления в оптическом волокне в каналах Алисы и Боба в зависимости от средней квадратической погрешности $\sigma = \sigma_\omega$ углов ω_A и ω_B

Формула для среднего значения вероятности $P_{\text{err}}^{\text{BF}}$ имеет вид

$$\overline{P}_{\text{err1}}^{\text{BF}} = \frac{1}{4} - \frac{1}{8}\Bigg(\left(1 + \exp\left(-4\sigma_\theta^2\left(1 - r_\theta\right)\right)\right) \times \\ \times \left(\frac{1}{2} - \exp\left(-\frac{\sigma_\omega^2}{2}\right) + \frac{1}{2}\exp\left(-\sigma_\omega^2\right)\operatorname{ch}\left(\sigma_\omega^2 r_\omega\right)\right) + \\ + \exp\left(-\sigma_\theta^2\left(1 - r_\theta\right)\right)\exp\left(-\sigma_\omega^2\right)\operatorname{sh}\left(\sigma_\omega^2 r_\omega\right) + 2\exp\left(-\frac{\sigma_\omega^2}{2}\right)\Bigg).$$

Формула для среднего значения вероятности $P_{\text{err}}^{\text{F}}$ имеет вид

$$\overline{P}_{\text{err1}}^{\text{F}} = \frac{1}{4}\left(1 - \exp\left(-\sigma_\omega^2\left(1 - r_\omega\right)\right)\right). \tag{6}$$

Во втором случае предположим, что Алиса контролирует свой канал, и в ее канале отсутствуют ошибки. В этом случае в формулах (4) и (5) следует положить $\omega_A = 0$. В этом случае $P_{\text{err}}^{\text{BF}} = P_{\text{err}}^{\text{F}}/2$, и вероятность $P_{\text{err}}^{\text{BF}}$ не зависит от углов θ_A, θ_B. Усредненные по углу ω_B вероятности $P_{\text{err}}^{\text{BF}} = P_{\text{err}}^{\text{F}}/2$ имеют вид

$$\overline{P}_{\text{err}}^{\text{BF}} = \frac{\overline{P}_{\text{err}}^{\text{F}}}{2} = \frac{1}{8}\left(1 - \exp\left(-\frac{\sigma_\omega^2}{2}\right)\right). \tag{7}$$

Заключение

Используем правило подсчета вероятности Бернулли, получим соотношение для средней относительной ошибки (QBER) в переданном квантовом ключе (среднее число ошибок в просеянном ключе длиной $N/2$ по отношению к длине просеянного ключа): $\text{QBER} = 2\overline{P}_{\text{err}}$. В работе рассмотрены две оптимальные стратегии выбора отрезков OB с целью минимизации средних ошибок в просеянном ключе. В первом случае при наличии в двух квантовых каналах двулучепреломления с равными дисперсиями σ_ω^2 углов ω_A и ω_B и с равными дисперсиями σ_θ^2 углов θ_A и θ_B целесообразно подбирать отрезки OB с учетом корреляции по углам θ_A и θ_B.

При условии $\sigma_\theta^2(1 - r_\theta) \ll 1$ средняя вероятность ошибки в передаче кубита близка к

$$\frac{1}{4}(1 - \exp(-\sigma_\omega^2(1 - r_\omega))), \tag{8}$$

и при коррелированном выборе пар по углам ω_A и ω_B вероятность ошибки может стать малой при наличии двулучепреломления. Оптическая активность компенсируется при коррелированном выборе пар по углам ω_A и ω_B (6). На рис. 2 приведены графики средней ошибки QBER (8) в зависимости от средней квадратической погрешности $\sigma = \sigma_\omega$. Графики 1, 2, 4 на рис. 2 построены для коэффициентов корреляции $r = r_\omega = 0.98,\ 0.8,\ 0.3$ соответственно. Во втором случае, когда случайных ошибок в одном из каналов нет $(\omega_A = 0)$, исчезает зависимость вероятности ошибки в передаче кубита от угла θ_A, θ_B. Но для компенсации ошибок при флуктуации углов ω_A, ω_B необходим выбор ОВ с малой дисперсией σ_ω^2. В этом случае QBER рассчитывается по формуле

$$\mathrm{QBER} \approx \frac{1}{4}\left(1 - \exp\left(-\frac{\sigma_\omega^2}{2}\right)\right). \tag{9}$$

Зависимость (9) представлена на рис. 2, график 3. Как следует из рисунка, коррелированный выбор отрезков ОВ для каналов Алисы и Боба существенно изменяет среднюю ошибку QBER, делая ее ниже критического значения, равного 0.11, что позволяет применять распределенный ключ для целей криптографии.

Работа поддержана в рамках Аналитической ведомственной целевой программы «Развитие научного потенциала высшей школы» (№ 2.1.1/9425), Федеральной целевой программой «Научные и научно-педагогические кадры инновационной России» 2009–2013 годы (гос. контракт № П689; проект НК-526П/24) и НИОКР РК10186.

Summary

G.P. Miroshnichenko, A.A. Sotnikova. Error Compensation in Quantum Key Distribution Using Entangled Biphoton Polarization States.

We consider optimal strategies for selecting optical fiber segments for Alice and Bob's quantum channels that are used for quantum key distribution by entangled biphoton polarization states. We show that the quantum bit error rate in a sifted key can be substantially reduced, even with large dispersions in the random parameters of optical fiber. To do this, Alice and Bob's channels should be designed from fibers manufactured using the same technology. The selection of the pairs of optical fiber segments should be correlated, with a correlation coefficient close to 1.

Keywords: quantum cryptography, EPR-protocol, quantum bit error rate, optical fiber.

Литература

1. *Rashleigh S.C., Ulrich R.* High birefringence in tension-coiled single-mode fibers // Opt. Lett. – 1980. – V. 5, No 8. – P. 354–356.
2. *Menyuk C.R., Wai P.K.A.* Polarization evolution and dispersion in fibers with spatially varying birefringence // J. Opt. Soc. Am. B. – 1994. – V. 11, No 7. – P. 1288–1296.
3. *Poole C.D.* Statistical treatment of polarization dispersion in single-mode fiber // Opt. Lett. – 1988. – V. 13, No 8. – P. 687–689.
4. *Poole C.D., Winters J.H., Nagel J.A.* Dynamical equation for polarization dispersion // Opt. Lett. – 1991. – V. 16, No 6. – P. 372–374.

5. *Poppe A., Fedrizzi A., Ursin R., Bohm H.R., Lorunser T., Maurhardt O., Peev M., Suda M., Kurtsiefer C., Weinfurter H., Jennewein T., Zeilinger A.* Practical quantum key distribution with polarization entangled photons // Opt. Express. – 2004. – V. 12, No 16. – P. 3865–3871.

6. *Muller A., Zbinden H., Gisin N.* Quantum cryptography over 23 km in installed underlake telecom fibre // Europhys. Lett. – 1996. – V. 33, No 5. – P. 335–339.

Поступила в редакцию
05.04.11

Мирошниченко Георгий Петрович – доктор физико-математических наук, профессор кафедры высшей математики, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия.

E-mail: *gpmirosh@gmail.com*

Сотникова Анна Андреевна – аспирант кафедры высшей математики, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия.

E-mail: *oirt@yandex.ru*