

ПОГРЕШНОСТИ В «ПРОСЕЯННОМ» КВАНТОВОМ КЛЮЧЕ ПРИ ЕГО ПЕРЕДАЧЕ ПО ОДНОМОДОВОМУ СТОХАСТИЧЕСКОМУ АНИЗОТРОПНОМУ НЕОДНОРОДНОМУ ОПТОВОЛОКНУ

Г. П. Мирошниченко¹, А. А. Сотникова

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

¹gpmirosh@gmail.com

Рассмотрена динамика во времени полевой матрицы плотности в базисе состояний вакуума и двух ортогональных поляризаций фотонов. В качестве анализатора использован прибор с пассивной модуляцией состояний распределяемых фотонов и с невозбужденными вспомогательными модами. Ошибки в просеянном ключе могут возникать из-за поглощения и деполяризации фотонов и разброса параметров оптического волокна (ОВ). Найдена средняя по разбросу параметров ОВ относительная ошибка (QBER) в просеянном квантовом ключе, распределенном по протоколу BB84 с поляризационным кодированием информации. Показано, что QBER можно существенно уменьшить, даже при больших дисперсиях случайных параметров ОВ. Найдены условия работы протокола на больших расстояниях, для этого используется эффект поляризационного бие-ния, который явно выражен, когда среднее значение параметров ОВ превосходит их разброс. Сделан вывод о том, что правильный выбор технологии изготовления ОВ позволит снизить QBER до критического уровня, равного 0.11, ниже которого распределенный ключ можно использовать для целей криптографии.

Ключевые слова: квантовая криптография, шумы в квантовом канале, QBER, оптическое волокно, фотоны, ошибка в квантовом ключе, поляризационное кодирование информации.

1. Введение

Новым направлением современной информатики (науки о методах передачи, хранения и обработки информации) являются оптические квантовые информационные технологии. Квантовая информатика ставит перед теорией передачи информации по квантовому каналу новые задачи. Оптическое волокно (ОВ) используется как информационный канал для передачи классической информации, закодированной с помощью модуляции физических характеристик электромагнитной волны, таких как амплитуда, частота, фаза, поляризация. Теория распределения квантовой информации по ОВ должна быть основана на законах квантовой механики и квантовой оптики. В шредингеровском представлении для описания развития во времени матрицы плотности фотонов $\rho(t)$ необходим гамильтониан оптических мод (фотонов) в одномодовом ОВ, в котором могут распространяться две, перпендикулярно поляризованные волны, фазовый фронт которых близок к плоскому (мода HE_{11}). Для электромагнитной волны ОВ представляет собой неоднородную стохастическую анизотропную среду. Стохастичность среды и квантовые шумы в канале приводят к декогеренции (деполяризации) квантовых состояний фотонов и поглощению фотонов. Просеянный квантовый ключ, переданный по ОВ, содержит ошибки. В литературе степень секретности характеризуют синтетическим параметром — скоростью появления ошибок в квантовых битах (английская аббревиатура QBER) [1], [2], [3]. QBER зависит от различных физических свойств квантового канала, передатчика, приемника, стратегии перехвата

и других характеристик. В частности, QBER зависит от относительной ошибки в квантовом ключе, оставшейся после этапа просеивания. Ошибки в квантовом ключе могут быть обнаружены в процессе процедуры исправления ошибок и усиления секретности. Эти процедуры занимают время, и приводят к потере части переданного ключа. Правильный выбор технологии изготовления оптоволоконного квантового канала позволит снизить ошибки при распределении квантового ключа.

2. Преобразование матрицы плотности фотонов в анизотропном неоднородном одномодовом ОВ

Гамильтониан взаимодействия мод (обобщение классического метода связанных волн) имеет вид

$$\hat{V} = \sum_{\mathbf{k}, \mu, \mu' = H, V} \frac{1}{2} (\xi, \sigma)_{\mu, \mu'} \cdot \hat{b}_{\mathbf{k}\mu}^\dagger \hat{b}_{\mathbf{k}\mu'}. \quad (1)$$

Здесь ξ — вещественный вектор, характеризующий взаимодействие ортогонально поляризованных мод с волновым вектором k . Изучим преобразование состояния поля при распространении фотона в ОВ. В качестве базисных состояний выберем три вектора $|0\rangle, |1\rangle, |2\rangle$ (здесь $|0\rangle$ — вакуумное состояние моды, которое необходимо включать в рассмотрение для учета поглощения)

$$|1\rangle = |H\rangle = \hat{b}_{\mathbf{k}\mu=H}^\dagger |0\rangle, \quad |2\rangle = |V\rangle = \hat{b}_{\mathbf{k}\mu=V}^\dagger |0\rangle.$$

С течением времени полевое состояние изменяется согласно квантовому уравнению Лиувилля для шредингеровской матрицы плотности фотонов

$$\frac{\partial \rho(t)}{\partial t} = -i [\hat{V}, \rho(t)] + \hat{\Gamma} \rho(t), \quad \rho(0) = \rho_0. \quad (2)$$

Здесь $\hat{\Gamma}$ — супероператор релаксации, а $\rho(t)$ — матрица плотности фотона в момент времени t . Матрица плотности определяется четырьмя вещественными и двумя комплексными функциями $P(t), \rho_{01}(t), \rho_{02}(t), \mathbf{p}(t)$:

$$\begin{aligned} \rho(t) = & (1 - P(t)) |0\rangle\langle 0| + (\rho_{01}(t) \cdot |0\rangle\langle 1| + \rho_{02}(t) \cdot |0\rangle\langle 2| + \{H.C\}) + \\ & + \frac{1}{2} (P(t) (|1\rangle\langle 1| + |2\rangle\langle 2|) + (\mathbf{p}(t), \sigma)) \end{aligned}$$

Предполагается, что характер релаксации изотропный, учитывается поглощение фотонов, может стремиться к нулю степень поляризации поля (длина вектора $\mathbf{p}(t)$). Система уравнений для функций $P(t), \rho_{01}(t), \rho_{02}(t), \mathbf{p}(t)$ имеет вид

$$\begin{cases} \frac{d}{dt} P(t) = -\delta \cdot P(t), \\ \frac{d}{dt} \rho_{01}(t) = -\left(\frac{i}{2} \xi_z + \gamma_{01}\right) \rho_{01}(t) + \frac{i}{2} (\xi_x + i \xi_y) \rho_{02}(t), \\ \frac{d}{dt} \rho_{02}(t) = -\left(\frac{i}{2} \xi_z + \gamma_{02}\right) \rho_{02}(t) + \frac{i}{2} (\xi_x - i \xi_y) \rho_{01}(t), \\ \frac{d}{dt} \mathbf{p}(t) = [\xi \times \mathbf{p}(t)] - \hat{\gamma} \cdot \mathbf{p}(t). \end{cases}$$

Здесь введены феномологические скорости поглощения и деполяризации. Естественно предположить изотропный механизм деполяризации

$$\hat{\gamma}_{\alpha, \beta} = (\delta + \gamma) \delta_{\alpha, \beta}, \quad \delta + \gamma \geq \delta \geq 0,$$

$\delta + \gamma$ — скорость деполяризации, δ — скорость поглощения фотонов, γ_{01}, γ_{02} — скорости разрушения корреляций с вакуумом. Решение системы уравнений имеет вид

$$\begin{aligned} P(t) &= \exp(-\delta t) P(0), \\ \rho_{01}(t) &= c_1 \exp\left(-\frac{2\gamma_{01} + \sqrt{i(\xi_z^2 - \xi_x^2 - \xi_y^2)}}{2}t\right) + c_2 \exp\left(-\frac{2\gamma_{01} - \sqrt{i(\xi_z^2 - \xi_x^2 - \xi_y^2)}}{2}t\right), \\ \rho_{02}(t) &= \frac{1}{\xi_x + i\xi_y} \left(i\xi_z \rho_{01}(t) + 2\gamma_{01} \rho_{01}(t) + 2\overline{\rho_{01}(t)} \right), \\ \mathbf{p}(t) &= \exp(-(\delta + \gamma)t) W(\xi, t) \mathbf{p}(0). \end{aligned}$$

Здесь $W(\xi, t)$ — матрица преобразования вектора при повороте системы координат на угол $\omega = \xi t$ вокруг оси $\mathbf{n}$, где $\xi = \xi \mathbf{n}$. В качестве анализатора используем прибор с пассивной модуляцией с вакуумными вспомогательными модами, изображенный на рис. 1. Расчет показывает, что вероятности P_1, P_2, P_3, P_4 срабатывания детекторов D_1, D_2, D_3, D_4 записываются через найденные решения

$$P_1 = \frac{P(t) + \mathbf{p}_z(t)}{4}, \quad P_2 = \frac{P(t) + \mathbf{p}_x(t)}{4}, \quad P_3 = \frac{P(t) - \mathbf{p}_z(t)}{4}, \quad P_4 = \frac{P(t) - \mathbf{p}_x(t)}{4}.$$

Будем считать, что Алиса с равной вероятностью $1/4$ генерирует одно из четырех состояний и посылает их Бобу на анализатор через шумящий канал (учитываем возможный вклад вакуумного состояния):

$$\begin{aligned} |\Psi^{(1)}\rangle &= \alpha|0\rangle + \beta|1\rangle, \quad |\Psi^{(2)}\rangle = \alpha|0\rangle + \frac{\beta}{\sqrt{2}}(|2\rangle + |1\rangle), \\ |\Psi^{(3)}\rangle &= \alpha|0\rangle + \beta|2\rangle, \quad |\Psi^{(4)}\rangle = \alpha|0\rangle + \frac{\beta}{\sqrt{2}}(|2\rangle - |1\rangle). \end{aligned}$$

Для этих состояний начальные данные имеют вид

$$\begin{aligned} P(0) &= |\beta|^2, \quad \mathbf{p}^{(1)}(0) = |\beta|^2 \mathbf{e}_z, \quad \mathbf{p}^{(4)}(0) = -\mathbf{p}^{(2)}(0), \\ \mathbf{p}^{(2)}(0) &= |\beta|^2 \mathbf{e}_x, \quad \mathbf{p}^{(3)}(0) = -\mathbf{p}^{(1)}(0). \end{aligned}$$

Расчет показывает, что полная вероятность ошибки при передаче одного (любого) кубита равна

$$\begin{aligned} P_{err} &= \frac{1}{4} \left(P(t) - \frac{\mathbf{p}_z^{(1)}(t) + p_x^{(2)}(t)}{2} \right) = \\ &= \exp(-\delta t) \frac{|\beta|^2}{4} \left(1 - \frac{W_{x,x}(\xi, t) + W_{z,z}(\xi, t)}{2} \exp(-\gamma t) \right). \end{aligned}$$

Средняя длина просеянного ключа N_{sift} , выраженная через N — полное число посылок.

$$N_{sift} = \frac{N}{2} P_{det} = \frac{N}{2} |\beta|^2 \exp(-\delta t).$$

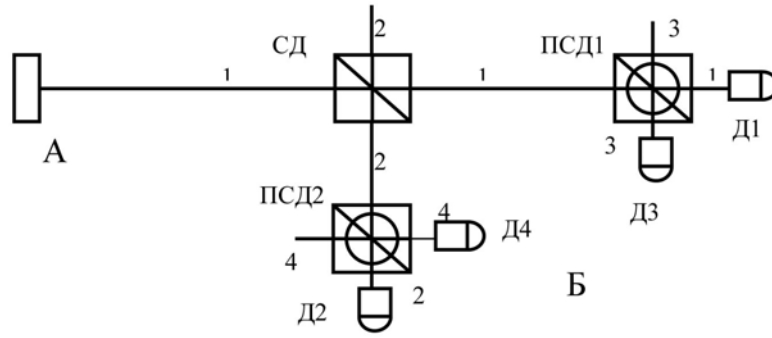


Рис. 1. Схема установки распределения квантового ключа по протоколу BB84. А – передатчик Алисы, Б – анализатор Боба, СД – светоделитель, ПСД1 – поляризационный светоделитель (пропускается состояние $|H\rangle$, отражается состояние $|V\rangle$), ПСД2 – поляризационный светоделитель (пропускается состояние $\frac{|H\rangle+|V\rangle}{\sqrt{2}}$, отражается состояние $\frac{|H\rangle-|V\rangle}{\sqrt{2}}$), Д1, Д2, Д3, Д4 – фотодетекторы. Цифрами пронумерованы входы и выходы светоделителей

3. Учет стохастичности параметров ОВ

Будем полагать, что плотность вероятности компонент случайного вектора параметров оптоволокна ξ имеет вид

$$\Omega(\xi) = \frac{1}{\sigma^3 (2\pi)^{3/2}} \exp\left(-\frac{|\xi - \bar{\xi}|^2}{2\sigma^2}\right).$$

Средний вектор Блоха-Стокса имеет вид

$$\bar{\mathbf{p}}(t) = \exp(-(\delta + \gamma)t) \bar{W}(\xi, t) \mathbf{p}(0), \quad \bar{W}(\xi, t) = \iiint \Omega(\xi) W(\xi, t) dV_\xi.$$

Упрощенное выражение для матрицы $W(t)$ получим в двух случаях. Первый случай – $\bar{\xi} > \sigma$ – сильное взаимодействие мод, малый разброс параметров ОВ. Тогда, в старшем порядке по параметру $\sigma/\bar{\xi}$

$$\bar{W}(t)_{x,x} \approx \cos(\bar{\xi}t) \exp\left(-\frac{(\sigma t)^2}{2}\right), \quad \bar{W}(t)_{z,z} \approx 1. \quad (3)$$

Второй случай – $\bar{\xi} < \sigma$ – малое взаимодействие мод по отношению к разбросу параметров ОВ. Тогда, в старшем порядке по параметру $\bar{\xi}/\sigma$

$$\bar{W}(t)_{x,x} \approx \bar{W}(t)_{z,z} \approx \frac{1}{3} \left(1 + 2(1 - (\sigma t)^2) \exp\left(-\frac{(\sigma t)^2}{2}\right) \right). \quad (4)$$

Оценим зависимость средней по ансамблю отрезков ОВ вероятности ошибки в передаче кубита информации по протоколу BB84 от параметров.

4. Обсуждение результатов и 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): $QBER = \frac{N \cdot P_{err}}{N_{sift}}$.

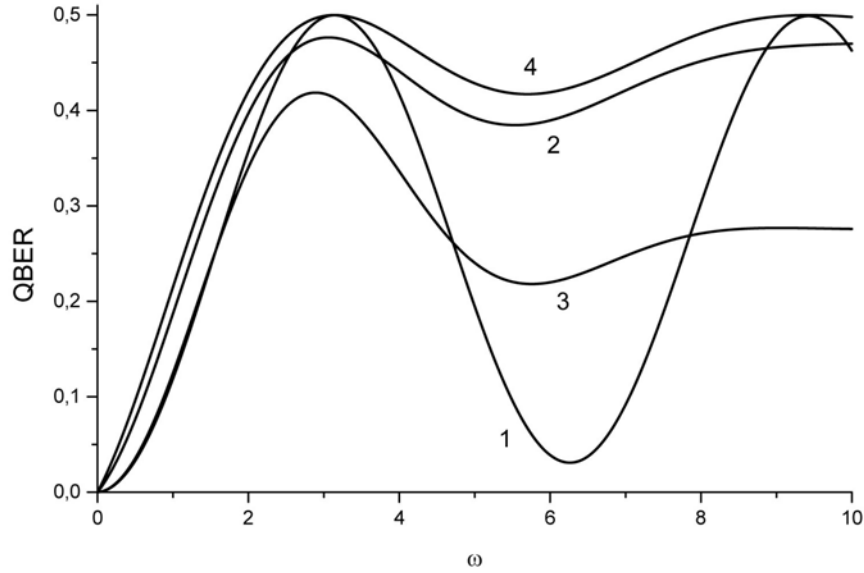


Рис. 2. Зависимость средней относительной ошибки в просеянном квантовом ключе QBER при условии $\sigma/\bar{\xi} \ll 1$ в зависимости от угла $\omega = \bar{\xi}t$, здесь σ — среднее квадратичное отклонение параметров оптоволокну, t — время задержки сигнала в квантовом канале, $\bar{\xi}$ — среднее значение модуля векторного параметра оптоволокну, γ — скорость деполяризации излучения. Кривая 1 — $\sigma/\bar{\xi} = 0.01$, $\gamma/\bar{\xi} = 0.01$; кривая 2 — $\sigma/\bar{\xi} = 0.2$, $\gamma/\bar{\xi} = 0.2$; кривая 3 — $\sigma/\bar{\xi} = 0.3$, $\gamma/\bar{\xi} = 0.01$; кривая 4 — $\sigma/\bar{\xi} = 0.01$, $\gamma/\bar{\xi} = 0.3$

На рис.2 зависимость средней относительной ошибки от угла рассчитана по формуле

$$QBER = \frac{1}{2} \left(1 - \frac{1}{2} \left(1 + \cos(\omega) \cdot \exp \left(-\frac{1}{2} \left(\frac{\sigma}{\bar{\xi}} \omega \right)^2 \right) \right) \exp \left(-\frac{\gamma}{\bar{\xi}} \omega \right) \right). \quad (5)$$

Как известно, QBER не должен превышать 0.11, в противном случае секретность квантового ключа не гарантируется. Как следует из рис. 2, при условии $\sigma \ll \bar{\xi}$ такое значение QBER достигается при малых значениях $\omega = \bar{\xi}t \ll 1$ и при больших значениях $\omega = \bar{\xi}t \approx 2\pi$, при условии $\gamma/\bar{\xi} < 0.04$.

На рис. 3 зависимость средней относительной ошибки от угла рассчитана по формуле

$$QBER = \frac{1}{2} \left(1 - \frac{1}{3} \left(1 + 2(1 - \omega^2) \exp \left(-\frac{\omega^2}{2} \right) \right) \exp \left(-\frac{\gamma}{\sigma} \omega \right) \right). \quad (6)$$

5. Выводы

В работе рассмотрена динамика во времени однофотонной матрицы плотности в базисе состояний с ортогональными поляризациями.

Найдена средняя по разбросу параметров ОВ относительная ошибка (QBER) в просеянном квантовом ключе, распределенном по протоколу BB84 с поляризационным кодированием информации.

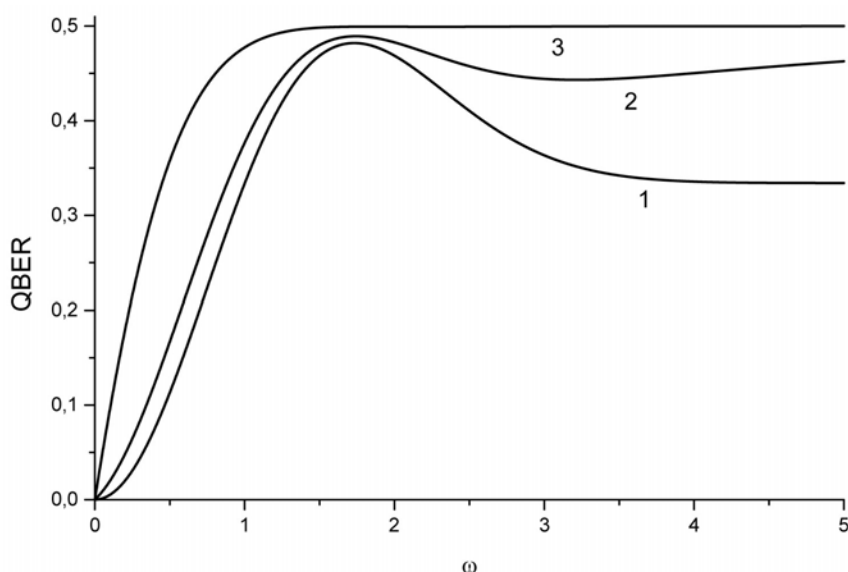


РИС. 3. Зависимость средней относительной ошибки в просеянном квантовом ключе QBER при условии $\bar{\xi}/\sigma \ll 1$ в зависимости от угла $\omega = \sigma t$, здесь σ — среднее квадратичное отклонение параметров оптоволокна, t — время задержки сигнала в квантовом канале, $\bar{\xi}$ — среднее значение модуля векторного параметра оптоволокна, γ — скорость деполяризации излучения. Кривая 1 — $\gamma/\sigma = 0.001$; кривая 2 — $\gamma/\sigma = 0.3$; кривая 3 — $\gamma/\sigma = 2$. QBER не превышает 0.11 при условии $\omega = \sigma t \ll 0.5$

В работе сделан вывод о том, что правильный выбор технологии изготовления ОВ квантового канала позволит снизить QBER до критического уровня, равного 0.11, ниже которого распределенный ключ можно использовать для целей криптографии.

Работа поддержана АВЦП «Развитие научного потенциала высшей школы (2009-2011 годы)» (проект № 2.1.1/9425), ФЦП «Научные и научно-педагогические кадры инновационной России на 2009-2013 годы» (контракты НК-526Р, 14.740.11.0879, 16.740.11.0030), грантом 11-08-00267 РФФИ.

Литература

- [1] Castelletto S., Degiovanni I. P., Rastello M. L. Quantum and classical noise in practical quantum-cryptography systems based on polarization-entangled photons // Phys. Rev. A. — 2003. — 67. — P. 022305.
- [2] Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Rev. Mod. Phys. — 2002. — 74. — P. 145–195.
- [3] Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dusek M., Lutkenhaus N., Peev M. The security of practical quantum key distribution // Rev. Mod. Phys. — 2009. — 81. — P. 1301–1350.