УДК 621.373

КВАНТОВАЯ КРИПТОГРАФИЯ НА ФОТОННЫХ ПАРАХ, ПЕРЕПУТАННЫХ ПО ВОЛНОВЫМ ВЕКТОРАМ

© 2004 О.Р. Ерёмина, В.И. Игошин

Самарский филиал Физического института им. П.Н. Лебедева РАН

Проведен анализ квантовой модели преобразования лазерной накачки в фотонные пары, перепутанные по волновым векторам в нелинейном кристалле β-BBO. Определены требования к параметрам лазерной накачки для планируемых экспериментов по квантовой криптографии. Расчеты показывают, что наиболее приемлемая длительность импульса лежит в диапазоне нескольких десятков фемтосекунд, а радиус фокусировки r=0.015 мм. Таким образом, необходимая энергия импульса должна превышать 30 мкДж. Для покадровой передачи изображений, когда частота следования импульсов около 10 Гц, средняя мощность лазерного накачки довольно мала и лежит в диапазоне микроватт. Для передачи ТВ изображения, когда $f=10^7$Гц , лазерная мощность должна превышать 0.3 Вт.

Состояние исследований в области квантовой криптографии

В современном мире передача конфиденциальных данных между несколькими абонентами в различных сетях связи может привести как к потере передаваемой информации, так и к ее компрометации. Все криптографические системы основаны на использовании криптографических ключей. Чем больше ключ, тем сложнее его подобрать обычным простым перебором. Для вскрытия современной криптосистемы со средней длиной ключа потребуется около 10^{50} машинных операций, что практически невозможно на современных компьютерных системах. Наиболее известные симметричные криптосистемы – шифр Цезаря, шифр Вижинера, американский стандарт шифрования DES, шифр IDEA и отечественный стандарт шифрования данных ГОСТ 28147-89. Асимметричные криптосистемы предполагают использование двух ключей - открытого и секретного. Схему асимметрической криптографии в 1976 г. предложили два молодых американских математика Диффи и Хеллман. Наиболее известные асимметричные криптосистемы это шифр RSA и шифр Эль Гамаля. Безопасность любого криптографического алгоритма определяется используемым криптографическим ключом. Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей. Как правило, применяют датчики псевдослучайных чисел. Однако степень случайности генерации чисел должна быть достаточно высокой. Идеальными генераторами являются устройства на основе натуральных случайных процессов, например на основе белого шума. В результате развития квантовых компьютеров и квантовой криптографии на свет появился квантовый криптоанализ. Он обладает неоспоримыми преимуществами. Возьмем, к примеру, известный и распространенный ныне шифр RSA (Rivest, Shamir, Adleman, 1977). В основе системы RSA лежит предположение о том, что решение математической задачи о разложении больших чисел на простые множители на классических компьютерах невозможно – оно требует экспоненциально большого числа операций и астрономического времени. Для решения этой задачи был разработан квантовый алгоритм, который дает возможность вычислить простые множители больших чисел за практически приемлемое время и взломать шифр RSA. Таким образом, для RSA квантовый компьютер, а следовательно, квантовый криптоанализ - крайне плохая новость. Бурное развитие квантовых технологий и волоконно-оптических линий связи привело к появлению квантово-криптографических систем. Они являются предельным случаем защищенных волоконно-оптических линий

связи (ВОЛС). Использование квантовой механики для защиты информации позволяет получать результаты, недостижимые как техническими методами защиты ВОЛС, так и традиционными методами математической криптографии. Защита такого класса применяется в ограниченном количестве, в основном для защиты наиболее критичных с точки зрения обеспечения безопасности систем передачи информации в ВОЛС. Исследования показали, что попытка перехвата информации из квантового канала связи неизбежно приводит к внесению в него помех, обнаруживаемых законными пользователями этого канала. Квантовая криптография использует этот факт для обеспечения возможности двум сторонам, которые ранее не встречались и не обменивались никакой предварительной секретной информацией, осуществлять между собой связь в обстановке полной секретности без боязни быть подслушанными злоумышленником. Квантовый канал обмена информацией может быть осуществлен через лазерный пучок, распространяющийся в атмосфере или космосе.

В настоящее время уже во многих странах мира квантовые криптосистемы на базе ВОЛС реализованы экспериментально, а в некоторых странах введены в опытную эксплуатацию. В частности, в Лос-Аламосской национальной лаборатории завершена разработка и введена в опытную эксплуатацию в США линия связи общей длиной 48 км (4x12 км), в которой на принципах квантовой криптографии осуществляется распределение ключей со скоростью несколько десятков кбит/с.

В университете Дж. Хопкинса (США) реализована локальная вычислительная сеть с квантовым каналом связи длиной 1 км, в которой за счет оперативной автоматической подстройки каждые 10 мин достигнут низкий уровень ошибок в канале (0,5%) при скорости передачи 5 кбит/с.

В Великобритании, в Оксфордском университете, реализован ряд квантово-криптографических схем с использованием квантовых усилителей для повышения скорости передачи. Скорость передачи в квантовом канале по ряду причин очень низка. Применение квантовых усилителей как раз призвано способствовать преодолению существующих ограничений по скорости передачи в квантовом канале и резкому расширению диапазона возможных применений подобных систем

В Самарском филиале Физического института им. П.Н. Лебедева на протяжении последних трех лет проводится исследование оптической схемы квантового криптофакса – устройства, в котором осуществляется информационно защищенная передача изображений с использованием законов квантовой механики, а именно с использованием сцепленных состояний фотонов. Этим (передачей изображений) наши исследования отличаются от более традиционных схем квантовой криптографии, в которых осуществляется защищенная передача текстовых файлов. К настоящему времени нами разработана квантово-механическая модель генерации сцепленных по направлениям двухфотонных состояний и на этой основе определены требования к элементной базе устройства – лазеру, фотоприемникам. Эти результаты излагаются во второй части данной статьи. Подобные исследования проводятся и в США. В США проведены начальные эксперименты в этой области, показавшие принципиальную возможность создания квантового криптофакса.

Частным случаем информационно защищенной передачи изображения является защита текстовых файлов посредством перепутывания фотонов. Концептуальное основание для квантовой криптографии, основанной на перепутывании (сцепленности), обладает другой природой по сравнению с распределением ключа с одиночными поляризованными фотонами. Квантовое распределение ключа с поляризованными одиночными фотонами в настоящее время устарело, поскольку этот метод кодирования раскрывается когерентной квантовой атакой, разработанной в последнее время [1].

Перепутанные состояния необходимы для описания состояния совокупной системы, состоящей из нескольких частей, в том числе пространственно разделённых. Примером таких состояний может служить состоя-

ние квантовой системы, образованной двумя однофотонными пучками с различными волновыми векторами. Состояние фотонной пары представимо в виде суперпозиции базисных состояний:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\vec{k}\rangle_1 |\vec{k}'\rangle_2 + |\vec{k}'\rangle_1 |\vec{k}\rangle_2\right)|\vec{e}_1\rangle|\vec{e}_2\rangle,$$

где $\vec{k}$ и $\vec{k}'$ волновые векторы фотонов, $\vec{e}_1$ и $\vec{e}_2$ векторы поляризации.

Каждый фотон одного пучка связан с фотоном другого пучка и общее состояние не является произведением волновых функций отдельных фотонов. Перепутанные состояния обладают замечательным свойством: как только волновой вектор одного фотона становится известным в результате измерения, то волновой вектор второго фотона становится строго определенным. Сейчас это свойство доказано экспериментально и может быть положено в основу новых подходов к реализации квантовой криптографии.

Как защита текстовых файлов, так и защита изображений базируются на одной и той же технике эксперимента. Подслушивающий агент не может извлечь из частиц никакой информации на их пути от источника к законным пользователям, просто потому, что там никакой информации не закодировано. Информация рождается только после того, как перепутанные по волновым векторам пучки сходятся на детектирующем устройстве у законного пользователя.

Информационно-защищенная передача текстовых файлов и изображений с применением перепутанных (сцепленных) по волновым векторам фотонных пар является новым направлением в квантовой криптографии, отличным от уже отработанных схем квантовой криптографии, которые не защищены от новых квантовых схем атаки.

В настоящей работе разработана и проанализирована квантовомеханическая модель генерации сцепленных фотонных пучков для информационно защищенной передачи файлов. Квантовый криптофакс мыслится как устройство, в котором (рис. 1): а.) лазерный пучок от лазера параметрически преобразуется в два пучка с ортогональной поляризацией фотонов и уменьшенной вдвое энергией квантов; эти пучки делятся по направлениям с помощью поляризационного расщепителя пучка, но фотоны в них находятся в сцеплённых по волновым векторам состояниях; б) в один из пучков вводится маска и промодулированный пучок направляется в детектор D_1 ; в) второй пучок , находящийся в сцеплённом состоянии с первым, сканируется с помощью световода в поперечном сечении и излучение направляется на детектор D_2 , г) сигналы от D_1 и D_2 направляются на схему совпадений и от неё на компьютер , на дисплее которого возникает передаваемый файл. Такая передача данных является информационно защищённой, поскольку в канале от D_1 ,предположительно доступному для подслушивателя идёт беспорядочная последовательность импульсов. Значимая информация возникает в момент совпадений и доступна только принимающей стороне.

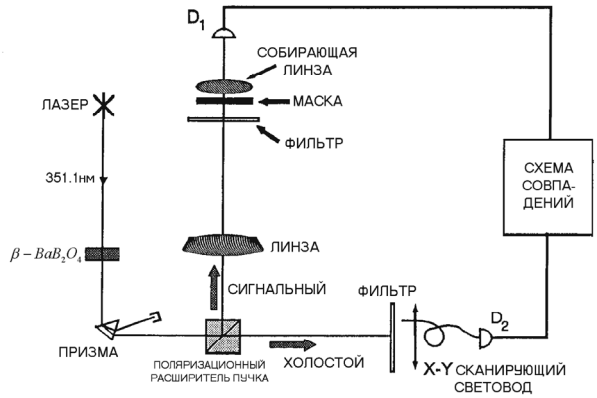

Рис. 1. Оптическая схема квантового криптофакса

Получение и управление квантово-перепутанными состояниями фотонов: расчет элементной базы планируемых экспериментов

Монохроматический световой пучок частоты ω_1, падающий на нелинейную среду, порождает поле на частоте гармоники $\omega_2 = 2\omega_1$. Гамильтониан параметрического процесса может быть записан в следующем виде[2]:

$$\hat{H} = \sum_{i=1}^{2} \hbar\omega_i (\hat{n}_i + \frac{1}{2}) + \hbar g \left[\hat{a}_1^{+}\, \hat{a}_2^{+}\, V_0 e^{-i\omega_0 t} + э.с. \right].$$

Решение квантовых уравнений движе-

ния [2] приводит к следующей формуле для среднего значения числа фотонных пар, рождающихся на выходе из кристалла BaB_2O_4:

$$\langle n(t) \rangle = sh^2(g|V_0|t),$$

где t-время взаимодействия волны с кристаллом.

В этой формуле неопределённым является параметр g. Параметр $V_0^{\,2}$ определяется энергетическими характеристиками лазера: это число фотонов, излученных за время лазерного импульса. Параметр g, заранее нам неизвестный, можно получить, исходя из принципа соответствия.

Нелинейное параметрическое взаимодействие в рамках классической электродинамики описывается следующими уравнениями для амплитуд полей [3]:

$$\begin{cases} \dfrac{dA_1}{dz} = -i\lambda\upsilon_\phi A_3 A_2^* \exp[-i\Delta kz], \\ \dfrac{dA_2}{dz} = -i\lambda\upsilon_\phi A_3 A_1^* \exp[-i\Delta kz]. \end{cases} \qquad (1)$$

Поле накачки A_3 считаем постоянным, поскольку эффективность преобразования мала. Входящий сюда параметр λ выражается через нелинейную восприимчивость [3]:

$$\lambda = \frac{d_{eff}}{c_0}\left(\frac{\omega_1\omega_2\omega_3}{n_1n_2n_3}\right)^{1/2}.$$

Нелинейная восприимчивость

$$d_{eff} = d_{ijk}(\varepsilon_{\omega_3 k_3})_i(\varepsilon_{\omega_1 k_1})_j^*(\varepsilon_{\omega_2 k_2})_k^*$$

для кристалла BaB_2O_4 вычисляется по матрице нелинейных восприимчивостей с учётом класса его симметрии 3m:

$$d_{ijk} = \begin{vmatrix} 0 & 0 & 0\ 0 & d_{24} & -d_{21} \\ -d_{21} & d_{21} & 0\, d_{24} & 0 & 0 \\ d_{31} & d_{31} & 0\ 0 & 0 & 0 \end{vmatrix}.$$

Зная тензор, составляющие векторов поляризации взаимодействующих волн на соответствующие оси $\varepsilon_{\omega_1 k_1}(\sin\varphi, -\cos\varphi, 0)$, $\varepsilon_{\omega_2 k_2}(-\cos\theta\cos\varphi, -\cos\theta\sin\varphi, \sin\theta)$, $\varepsilon_{\omega_3 k_3}(\sin\varphi, -\cos\varphi, 0)$, найдём выражение для эффективной нелинейной восприимчивости:

$$d_{eff} = d_{31}\sin\theta - d_{22}\cos\theta\sin 3\varphi,$$

где θ - угол между направлением распространения волны и оптической осью является углом синхронизма, при котором выполняется $\omega_1 + \omega_2 = \omega_3$, $\Delta k = 0$ и он находится из данных поверхностей нормали для обыкновенной и необыкновенной волны в кристалле. Согласно расчётам он равен 37^0. Угол φ выбирается так, чтобы эффективная нелинейная восприимчивость была максимальна. Для кристалла ВВО $d_{31} = \pm 0.16\cdot 10^{-12}$ м/В, $d_{22} = \pm 2.2\cdot 10^{-12}$ м/В [4], поэтому $d_{eff} = 0.16\cdot 10^{-11}$ м/В.

В квантовой оптике уравнения движения Гейзенберга для операторов сигнального и холостого фотонов таковы [2]:

$$\begin{cases} \dfrac{d\hat{A}_1(t)}{dt} = -igV_0\hat{A}_2^+(t) \\ \dfrac{d\hat{A}_2(t)}{dt} = -igV_0\hat{A}_1^+(t) \end{cases} \qquad (2)$$

где V_0 параметр накачки, g-константа, характеризующая нелинейную восприимчивость в кристалле, $\hat{A}_1(t), \hat{A}_2(t)$-медленно меняющиеся операторы.

На основе принципа соответствия мы можем приравнять коэффициенты в (1) и (2), имеющие размерность обратной секунды:

$$igV_0 = i\lambda v_\phi A_3,$$

тогда

$$g = \frac{\lambda v_\phi A_3}{V_0}, \qquad (3)$$

и

$$A_3 = 19 * \sqrt{(\frac{n_3}{\omega_3})} * \sqrt{\frac{P_L}{\pi r^2}} . \qquad (4).$$

Мощность падающего пучка должна превышать пороговую мощность, которая определяется чувствительностью фотодетекторов [5]:

$$\frac{\hbar\omega_{1,2}}{t} sinh^2(gV_0 t) \geq P_{th}$$

или

$$gV_0 = \frac{arcsin\, h\left(\sqrt{\frac{P_{th} t}{\hbar\omega_{1,2}}}\right)}{t} . \qquad (5).$$

Для однофотонной цифровой камеры, описанной в [6], пороговая мощность по нашим расчётам составляет $P_{th} = 3.12 * 10^{-12}$ Вт. Расчёт основан на том, что шумовой ток равен 16 электронам/(пикс·с) и образование одного электрона требует поглощения четырёх фотонов.

Комбинируя формулы (3) и (4) можно получить для пороговой мощности лазерного импульса выражение:

$$P_L = \frac{g^2 V_0^2 \pi c^2 n_1 n_2}{d_{eff} \omega_1 \omega_2 v_ф (1.9 * 10^4)^2} r^2 . \qquad (6).$$

В таблице 1 представлены импульсные пороговые мощности и энергии в импульсе для разных радиусов фокусировки и разных длительностей импульса. Из этих данных видно, что наиболее приемлемым является использование фемтосекундных лазеров и фокусировки r=0.015 мм. При этом необходимая энергия в импульсе составляет около 30 мкДж.

В таблице 2 для импульса с $\tau_{имп} = 70фс$ и радиусом пучка 0.015 мм представлен расчёт средней мощности $\bar{P}$ в зависимости от частоты повторения импульса. Из этих данных видно, что для передачи видимого изображения, когда f=10Гц средняя мощность весьма невелика и составляет доли микроватт, в то же время для передачи телевизионного изображения $f=10^7$Гц необходим лазер с $\bar{P}$=0.3 Вт.

Заключение

Проведен анализ модели преобразования излучения накачки в нелинейном кристалле β -бората бария в сцепленные фотонные пучки при различных условиях накачки. Определены требования к экспериментальной базе для планируемых экспериментов по квантовой криптографии. Наиболее приемлемым является использование фемтосекундных лазеров с радиусом фокусировки r=0.015 мм. При этом необходимая энергия в импульсе составляет около 30 мкДж. Для передачи движущегося изображения, когда f=10Гц, средняя мощность весьма невелика и составляет доли микроватт, в то же время для передачи телевизионного изображения $f=10^7$Гц необходим лазер с $\bar{P}$=0.3 Вт.

Таблица 1. Импульсные пороговые мощности и энергии в импульсе

r, мм	P_L, Вт	ε ,мкДж $\tau_{имп} = 3nc$	ε ,мкДж $\tau_{имп} = 70фс$
0.015	**$3.68*10^5$**	**1.1**	**0.025**
0.5	**$4.1*10^8$**	**1230**	**28.7**

Таблица 2. Расчет мощности

f, Гц	10	10^3	10^6	10^7	10^8
$\bar{P}$,Вт	$0.25*10^{-6}$	$0.025*10^{-3}$	0.025	0.257	2.57

СПИСОК ЛИТЕРАТУРЫ

1. *N. Gisin, G. Ribordy, W. Tittel, H. Zbinden*. Quantum cryptography // Reviews of modern physics.2002. Vol. 74. №1
2. *Л.Мандель, Э.Вольф*. Оптическая когерентность и квантовая оптика. М.:Физматлит, 2000.
3. *О.Звелто*. Принципы лазеров. М.: Мир, 1990.
4. Электронный архив нелинейных кристаллов компании Eksma, http://www.eksma.lt/en/main/products/1/42?PID=298.
5. *O. R.Eremina, V.I.Igoshin, R.R.Letfullin*. Quantum cryptography on the "entangled" two-photon states // SCI2002 Proceedings, Vol VII " Information Systems Development II», Orlando, Florida, july 14-18. 2002.
6. *B. M. Jost, A. V. Sergienko, A. F. Abouraddy, B. E. A. Saleh and M. C. Teich*. Spatial correlations of spontaneously down-converted photon pairs detected with a single-photon-sensitive CCD camera // Optics Express. 1998.Vol.3. № 2.

QUANTUM CRYPTOGRAPHY OF THE PHOTON PAIRS ENTANGLED ON THE WAVE VECTORS

© 2004 O.R. Eremina, V.I. Igoshin

Samara Branch of Physics Institute named for P.N. Lebedev of Russian Academy of Sciences

The analysis of the quantum model of transformation of the laser pumping into the photon pairs entangled on the wave vectors in the nonlinear в-BBO-crystal was undertaken.
The requirements to the parameters of the laser pumping were determined for the planned experiments on the quantum cryptography. Calculations show that the most reasonable pulse duration is in the range of several dickers of femtoseconds and the radius of focusing r=0.015mm. Thus, the necessary energy in a pulse must exceed 30 μJ. For transfer of the frame-by-frame movement, when the pulse frequency f is about 10 Hz, the mean pumping power is rather small and it is in the microwatt range. For transfer of TV image in case that f= 10^7 Hz the laser power must exceed 0.3 W.