С.Кулик, д.ф.-м.н., Физический факультет
МГУ им. М.В.Ломоносова

КВАНТОВАЯ КРИПТОГРАФИЯ

ЧАСТЬ 2*

Продолжение обзора физических принципов квантового распределения ключа раскрывает основные способы кодирования информации – кодирование по поляризации и по фазе.

ОСЛАБЛЕННЫЕ ЛАЗЕРНЫЕ ИМПУЛЬСЫ

Под импульсом будем понимать те фиксированные интервалы времени, в течение которых должен прийти фотон. Наиболее простое решение проблемы приготовления однофотонных фоковских состояний – это ослабление лазерных импульсов, поле которых находится в когерентном состоянии со средним числом фотонов N. Вероятность найти n фотонов в таком состоянии описывается распределением Пуассона:

$$P(n,N)=\frac{N^n}{n!}e^{-N}.$$

Соответственно, вероятность того, что в не пустом (т.е. с $n\neq 0$) импульсе содержится более одного фотона, равна

$$P(n>1\,|\,n>0,N)=\frac{1-P(0,N)-P(1,N)}{1-P(0,N)}=$$
$$\frac{1-\left[N^0e^{-N}/0!\right]-N^1e^{-N}/1!}{\left[N^0e^{-N}/0!\right]}=\frac{1-e^{-N}(1+N)}{1-e^{-N}}\approx N/2. \qquad (22)$$

Очевидно, что эта вероятность может быть сделана произвольно малой при уменьшении N. Однако в этом случае большинство импульсов окажется пустым! Действительно, при малых N

$$P(n=0)=\frac{N^0}{0!}e^{-N}\to 1-N.$$

Наличие пустых импульсов уменьшает скорость передачи битов: они не несут информации, следовательно, такие импульсы следует отбросить в протоколе. Уменьшение скорости обмена битами может быть компенсировано увеличением частоты повторения импульсов. В настоящее время в телекоммуникационных схемах используются частоты передачи порядка гигагерц. Однако на практике возникает другая серьезная проблема – темновые отсчеты детекторов. На длинах волн λ телекоммуникационной связи (1,55 и 1,3 мкм) в настоящее время используются полупроводниковые детекторы на основе индий-галий-арсенида, легированного фосфором (InGaAs:P), которые обладают высокими темновыми шумами. Поэтому такие детекторы стробируются – включаются чуть раньше ожидаемого времени прихода несущего информацию импульса, а выключаются чуть позже. Практически используется уровень ослабления, соответствующий приблизительно N=0,1, т.е. примерно лишь один из десяти посылаемых импульсов оказывается непустым. Из (22) следует, что 5% непустых импульсов содержат больше одного фотона – эти события в основном определяют уровень ошибок.

Упрощенная временная развертка событий в КК представлена на рис.3:

а) лазер генерирует световые импульсы, которые ослабляются до уровня 0,1 фотон/импульс и посылаются через волоконную линию на станцию Боба, где детектируются в ожидаемые моменты времени;

б) синхроимпульсы следуют с периодом T;

в) ослабленные до уровня 0,1 фотон/импульс световые импульсы;

г) электрические импульсы, стробирующие детектор;

д) электрические импульсы на выходе детектора: при квантовой эффективности 10% без учета потерь в линии остается около 1% от общего числа световых импульсов. Темновые отсчеты возникают в случайные моменты времени и являются паразитным сигналом, который требуется учитывать при работе любой системы КК.

* Часть 1 см.: Фотоника, 2010, №2.

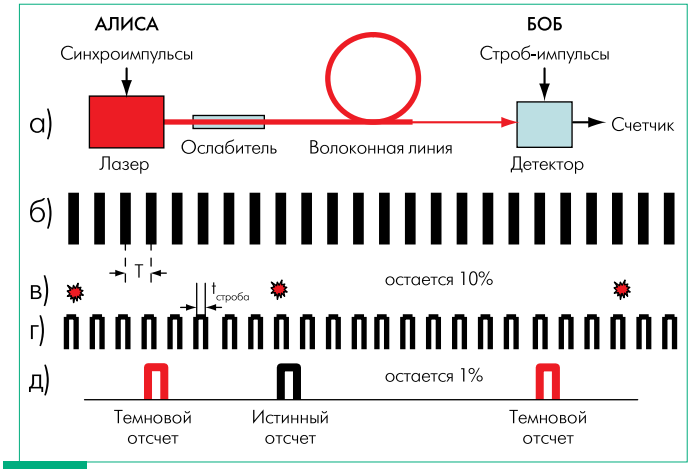

Рис.3 Упрощенная временная развертка событий в КК

ГЕНЕРАЦИЯ ДВУХФОТОННЫХ ИМПУЛЬСОВ

В другом способе получения псевдо-однофотонных состояний состоит в использовании пар фотонов, генерируемых при спонтанном параметрическом рассеянии (СПР) света. Один фотон при этом рассматривается как триггер для другого – так называемый генератор известного числа фотонов. Такой метод был предложен Д.Н.Клышко [21] и впервые был реализован в работе [22]. Второй детектор активизируется только после того, как первый детектор регистрирует фотон, поэтому, по определению, N = 1. Хотя в процессе СПР пары излучаются в случайные моменты времени, синхронизационная шкала теперь задается фотонами, давшими отсчет в первом детекторе. В типичных нелинейных кристаллах при мощности накачки 1 мВт удается получить около десятка миллионов пар в секунду в одной пространственно-частотной моде (имеется в виду одномодовый световод сечением несколько микрометров).

КОДИРОВАНИЕ

Говоря о практических реализациях КК, следует выделить два основных способа кодирования – кодирование по поляризации и фазе.

Кодирование по поляризации

Этот способ используется в основном при КК через открытое пространство. Действительно, при передаче по оптическому волокну изначально линейно поляризованный свет станет в общем случае поляризованным эллиптически на выходе из-за возникающих температурных и фазовых флуктуаций показателя преломления. Не смотря на то, что степень поляризации сохраняется (имеется в виду случай, когда длина когерентности света L_{eff} намного превышает эффективную длину волокна), любое чистое поляризационное состояние на выходе волокна будет подвержено сильным флуктуациям. Основные состояния при таком способе кодирования имеют вид:

$$|\updownarrow\rangle \equiv |V\rangle, |\leftrightarrow\rangle \equiv |H\rangle,$$

$$|\square\rangle = \frac{1}{\sqrt{2}}\{|H\rangle + |V\rangle\},$$

$$|\square\rangle = \frac{1}{\sqrt{2}}\{|H\rangle - |V\rangle\}, |\circlearrowright\rangle$$

$$|L\rangle \equiv \frac{1}{\sqrt{2}}\{|H\rangle + i|V\rangle\}, |\circlearrowleft\rangle$$

$$|R\rangle \equiv \frac{1}{\sqrt{2}}\{|H\rangle - i|V\rangle\}.$$

Они соответствуют вертикальной, горизонтальной, диагональным и (право- и лево) циркулярным поляризациям однофотонных фоковских состояний.

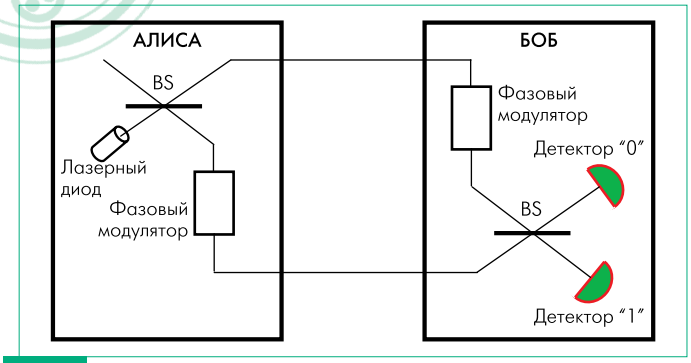

Рис.4 Схема фазового кодирования на основе сбалансированного интерферометра Маха-Цандера

Кодирование по фазе

Такой способ основан на использовании двухплечевого интерферометра Маха-Цандера (рис.4). Световые импульсы генерируются лазерным диодом и поступают в интерферометр. Интерферометр выполнен на оптическом волокне и включает в себя два симмметричных смесителя BS (аналог светоделителя), расположенных так, чтобы разность длин плеч была бы меньше длины когерентности. В обоих плечах, Алисы и Боба, находятся фазовые модуляторы. Число отсчетов однофотонных детекторов на станции Боба определяется изменением относительной фазы. Учитывая сдвиг фаз на 90 град. при отражении от светоделителя, набеги фаз в фазовых модуляторах Алисы и Боба, а также фиксированный набег фаз из-за разницы длин плеч, можно вычислить интенсивность в выходной моде "0" станции Боба:

$$I_0 = \bar{I}\cos^2\left(\frac{\phi_A - \phi_B + k\Delta L}{2}\right),$$

где $k=2\pi/\lambda$ – волновое число, а $\bar{I}$ – средняя интенсивность источника света. Если аргумент косинуса равен $\pi/2+\pi n$, n – целое, то в этой моде наблюдается деструктивная интерференция – весь свет направляется в моду "1". Если же аргумент косинуса равен πn, то весь свет направляется в моду "0". При промежуточных фазовых сдвигах свет регистрируется в обеих модах. Устройство в целом работает как оптический переключатель, причем важно поддерживать разность хода постоянной для наблюдения стабильной интерференции. На вход интерферометра подаются однофотонные состояния, полученные в одном из описанных выше методов.

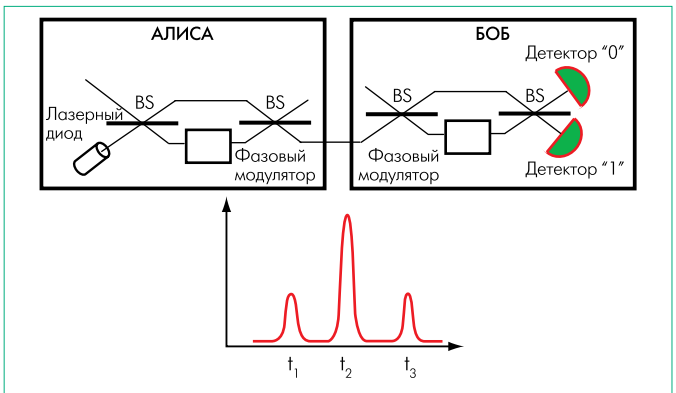

Рис.5 Схема КК на основе фазового кодирования и двух разбалансированных интерферометров Маха-Цандера

На практике удобнее использовать другую схему – два разбалансированных интерферометра Маха-Цандера (рис.5). Нетрудно заметить, что при использовании импульсного источника света временная функция распределения отсчетов в станции Боба будет содержать три пика. Первый соответствует тому, что и у Алисы и у Боба фотоны пошли через короткое плечо. Третий пик отвечает случаю, когда фотоны "выбрали" длинные пути. И, наконец, центральный пик соответствует ситуации, когда фотон Алисы пошел по короткому пути, а фотон Боба – по длинному, либо наоборот. Эти две последние ситуации неразличимы. На рис.5 справа показана функция распределения времен прихода фотонов. Центральный пик отвечает двум неразличимым случаям, когда фотон прошел по длинному плечу у Алисы и по короткому у Боба или по короткому у Алисы и по длинному у Боба.

Физически это значит, что разность длин плеч интерферометра Алисы должна быть такой же, как и у Боба, с точностью до длины когерентности света. Стабильность интерферометра за время передачи/приема должна быть на уровне долей длины волны света. Такая схема гораздо более стабильна. Однако остается проблема температурной стабилизации обоих интерферометров. Эта проблема является общей для обоих рассмотренных методов – поляризационного и фазового кодирования. Для ее решения необходима схема активной компенсации флуктуаций разности длин оптических плеч.

Простое решение проблемы состоит в том, чтобы иногда запускать в систему относительно интенсивные лазерные импульсы с N>>1, чтобы производить коррекцию фазовых или поляризационных искажений. Такие импульсы можно чередовать с ослабленными – квантовыми. Другой подход предусматривает пассивную компенсацию поляризационных флуктуаций в волокне на основе фарадеевского зеркала – именно так работают коммерческие схемы КК [23, 24].

КАНАЛЫ СВЯЗИ

Кроме квантового канала связи, по которому передающая и принимающая стороны обмениваются квантовыми состояниями – либо по волоконной оптической линии связи (ВОЛС), либо через атмосферу, – важным, неотъемлемым атрибутом КК является так называемый "открытый" канал связи. Открытым называется канал, если передаваемая по нему информация может быть доступна любому участнику протокола, в том числе злоумышленнику. Важным условием использования открытого канала в КК является невозможность изменить передаваемую по нему информацию. Таким каналом может выступать, например, Интернет.

ПРОТОКОЛЫ

Под протоколом понимается совокупность действий (таких как инструкции, команды, вычисления, алгоритмы), выполняемых в

заданной последовательности двумя или более легитимными субъектами с целью достижения некоего результата.

Известно несколько протоколов распределения ключей на основе дискретных квантовых состояний. В целом, их можно разбить на две группы. В первую входят протоколы КК, оперирующие с неортогональными квантовыми состояниями. Наиболее известные из них: BB84 [15], B92 [25], SARG [26]. Во вторую – протоколы, основанные на так называемых перепутанных квантовых состояниях и проверке выполнения соотношений типа неравенства Белла. Под перепутанными понимают состояния составной системы, волновую функцию которых (для чистых состояний) нельзя выразить через волновые функции подсистем. Другими словами, такое состояние составной системы полностью определено (оно описывается волновой функцией, и энтропия фон Неймана равна нулю), а состояния подсистем полностью неопределенны (они находятся в смешанном состоянии, и их энтропия достигает максимального значения). Наиболее известный протокол на перепутанных состояниях – протокол А.Экерта или E91 [27]. В основе отдельной группы протоколов КК лежит кодирование информации в квадратурные амплитуды моды квантованного электромагнитного поля [28, 29, 30].

В протоколе BB84 используется два (или, в общем случае, три) взаимно несмещенных базиса, состоящих из пары ортогональных состояний. Такие базисы удовлетворяют условию, что квадрат модуля скалярного произведения состояний из разных базисов равен обратной размерности гильбертова пространства:

$$\left|\left\langle \psi_i \middle| \varphi_j \right\rangle\right|^2 = 1/D,$$

в то время как для состояний из одного базиса скалярное произведение равно нулю:

$$\left\langle \psi_i \middle| \psi_j \right\rangle = 0 \ (i, j = 1, 2).$$

Так, при кодировании в поляризационных степенях свободы электромагнитного поля (D=2) можно составить три взаимно несмещенных базиса, которые образованы парами ортогональных поляризационных векторов:

лабораторный $\left(\left|\updownarrow\right\rangle \equiv \left|V\right\rangle, \left|\leftrightarrow\right\rangle \equiv \left|H\right\rangle\right)$,

диагональный $\left|\square\right\rangle \text{B} \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle \text{B} \left|V\right\rangle\right\}, \left|\square\right\rangle \text{B} \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle \text{B} \left|V\right\rangle\right\}$

и циркулярный $\left|L\right\rangle \equiv \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle + i\left|V\right\rangle\right\}, \left|R\right\rangle \equiv \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle - i\left|V\right\rangle\right\}.$

Полная формализация достигается, если состояниям, соответствующим вертикальной и горизонтальной поляризациям света, сопоставить векторы в т.н. лабораторном (или вычислительном) базисе: $\left|H\right\rangle \rightarrow \left|1\right\rangle, \left|V\right\rangle \rightarrow \left|0\right\rangle$. Протокол BB84 является наиболее популярным протоколом КК. В третьей части обзора мы рассмотрим его работу на примере поляризационных состояний фотонов.

ЛИТЕРАТУРА

21. **Клышко Д.Н.** – Квантовая электроника, 1977, 4.
22. **Rarity J.G., Tapster P. R., and Jakeman E.** Observation of sub-Poissonian Light in Parametric Downconversion. – Opt. Commun, 1987, 62, 201.
23. **Ribordy G., Gautier J. D., Gisin N. et al.** Automated 'plug & play' quantum key distribution.– Elec. Lett., 1998, 34, 2116-2117.
24. **Bourennane M., Gibson F., Karlsson B. A. et al.** Experiments on long wavelength (1550nm) "plug and play" quantum cryptography systems.– Optics Express, 1999, 4, 383.
25. **Bennett C.H.** Quantum cryptography using any two nonorthogonal states. –Phys. Rev. Lett., 1992, 68, 3121.
26. **Scarani V., Acin A., Ribordy G., and Gisin N.** Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. – Phys. Rev. Lett., 2004, 92, 057901.
27. **Ekert A.K.** Quantum cryptography based on Bell's theorem. – Phys. Rev. Lett., 1991, 67, 661.
28. **Grosshans F., G.Van Assche, Wenger J. et al.** Quantum Key Distribution using Gaussian-modulated Coherent States. –Nature, 2003, 421, 238.
29. **Fossier S., Diamanti E., Debuisschert T. et al.** A Field test of a continuous-variable quantum key distribution prototype. – New J. of Physics, 2009, 11, 045023.
30. **Elser D., Bartley T., Heim B. et al.** Feasibility of free space quantum key distribution with coherent polarization states. – New Journal of Physics 2009, 11, 045014.

Детектор фотонов

В апреле этого года ученые из Национального института стандартов и технологии США (NIST) объявили о создании однофотонного детектора, способного фиксировать единичные фотоны, передаваемые через волоконно-оптические кабели с эффективностью 99%. Этого достигают за счет повышенной согласованности детектора и оптических волокон. Принцип работы детектора заключается в использовании сверхпроводника как ультрачувствительного термометра. Каждый удар фотона повышает температуру датчика и увеличивает электрическое сопротивление. Отсутствие ложных срабатываний отличает его от других типов детекторов, имеющих очень высокий коэффициент усиления. Причина в том, что их уровень шума таков, что иногда шум ошибочно идентифицируется как фотон. Это приводит к погрешности в измерениях. Детектор предназначен для области электронной связи и квантовых измерений мощности оптического излучения.

www.photonics.com

Фемтосекундное будущее лазерной техники

Научная революция стартовала после появления принципиально нового источника света. 50 лет назад американский ученый Мейман продемонстрировал работу первого оптического квантового генератора. Признаным лидером лазерной тематики считался Басов. Он предлагал идеи, которые на первый взгляд выглядели фантастическими, а потом оказывались верными. Это идеи создания полупроводниковых лазеров, использования лазеров для управления термоядерным синтезом. Появлялись новые типы лазеров, увеличивалась их мощность, сокращалась длительность импульсов. Сначала был первый лазер на рубине, он давал доли микросекунды. Потом появились полупроводниковые лазеры. А потом, когда осуществили модуляцию добротности, лазеры перешли на наносекундный (10^{-9}) диапазон. С появлением неодимового стекла, в создании которого огромную роль сыграла ленинградская школа физики: Государственный оптический институт (ГОИ) и завод оптического стекла (ЛенЗОС), в Институте спектроскопии РАН освоили пикосекундный (10^{-12}) диапазон и вплотную подошли к фемтосекундам. В наши дни созданы фемтосекундные лазеры с длительностью импульсов порядка 10^{-15} с. Именно они и являются сейчас наиболее перспективными.

Фемтосекундные лазеры работают в двух режимах: выделив с помощью затвора одиночный ультракороткий импульс, его используют для исследования сверхбыстрых процессов, а, выделив из излучения единственную спектральную линию, получают источник света с исключительно высокой монохроматичностью и стабильностью интенсивности во времени, что используют в сверхточных оптических часах. За открытие в этой области ученым Холлу и Хэншу в 2005 году была присуждена Нобелевская премия. В ФИАНе под руководством Губина вместе с компанией "Авеста-проект" создают высокостабильные оптические часы с относительной нестабильностью всего 10^{-14}–10^{-15}. В их устройстве использован принцип сопряжения спектров Ne-Ne/CH4 и фемтосекундного волоконного лазера. Волоконные лазеры из стекла с примесями ионов редкоземельных металлов открывают путь к миниатюризации конечной установки, что важно в устройствах спутниковой навигации. Чичков (Лазерный центр Ганновера) с коллегами создали установку с фемтосекундным лазером, работающую на эффекте полимеризации материалов в жидкости под действием УФ-излучения. На сегодня в лазерах достигнута длительность импульса 5 фс.

По материалам интервью П.Крюкова АНИ "ФИАН-информ"