Письма в ЖЭТФ, том 78, вып. 10, с. 1156 – 1161

Экспериментальная схема квантовой криптографии на неортогональных состояниях с временным сдвигом и минимальным числом оптических компонентов

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия

Факультет вычислительной математики и кибернетики, Московского государственного университета им. М. В. Ломоносова, Москва, Россия

Поступила в редакцию 16 сентября 2003 г.

После переработки 7 октября 2003 г.

Описана новая схема для экспериментальной квантовой криптографии на неортогональных состояниях. Неортогональность достигается за счет временного сдвига состояний в различных посылках. Принципиальное преимущество данной схемы, например, по сравнению с наиболее развитой криптосистемой на принципе фазового кодирования, на которой достигнут рекорд по дальности, состоит в том, что в предлагаемой схеме для работоспособности достаточно точности балансировки плеч интерферометра на приемном и передающем концах в 1–2 см. Требуемая точность балансировки плеч интерферометра в схеме с фазовым кодированием составляет доли микрона на расстоянии в несколько десятков километров.

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

Квантовая криптография, или более точно – квантовое распространение ключа, позволяет реализовать абсолютно стойкую систему шифрования с одноразовыми ключами [1, 2]. Безусловно, секретное распространение ключа между пространственно удаленными легитимными пользователями гарантируется фундаментальными законами природы, а не ограниченными вычислительными или техническими возможностями подслушивателя. Безусловная секретность квантовой криптографии в нерелятивистской области[2)] базируется, по сути, на принципе неопределенностей Гейзенберга, более формально, – на невозможности одновременного измерения наблюдаемых, которые описываются некоммутирующими операторами. В терминах пары векторов состояний квантовой системы, в которые кодируется классическая информация о ключе, это означает невозможность получения любой информации о передаваемых квантовых состояниях без их возмущения, если последние являются неортогональными [3]. Другим фундаментальным запретом квантовой механики, тесно связанным с предыдущим, является запрет на копирование заранее неизвестного квантового состояния [4].

На сегодняшний день уже создано несколько различных прототипов квантовых криптосистем на базе оптоволоконных линий связи [5]. Рекорд дальности передачи секретного ключа в квантовой криптосистеме, с так называемой самокомпенсацией при помощи фарадеевских оптоволоконных отражателей, на сегодняшний день принадлежит японской (100 км)[6] и швейцарской группам (67 км) [7]. Имеющиеся прототипы квантовых криптосистем используют в основном следующие принципы: 1) информация о ключе кодируется в поляризационные степени свободы [8]; 2) фазовое кодирование, когда используются интерферометр Маха–Цандера, и информация кодируется в разность фаз, которая набирается на приемном и передающем плечах интерферометра [9, 10]; 3) квантовые криптосистемы с частотной модуляцией несущей частоты [11]; 4) квантовая криптография на когерентных состояниях с использованием гомодинного детектирования на приемном конце [12]. Наибольший прогресс достигнут в криптосистемах с фазовым кодированием и самокомпенсацией с использованием фарадеевских отражателей [6, 7, 13]. Упомянутые криптосистемы достаточно сложны в реализации. В данной работе предлагается новая квантовая криптосистема, которая, на наш взгляд, существенно проще уже имеющихся, и которая содержит минимальное число оптических оптоволоконных

[1)] e-mail: molotkov@issp.ac.ru

[2)] Под нерелятивистской квантовой криптографией всюду ниже понимается криптография, которая базируется лишь на геометрических свойствах векторов в гилбертовом пространстве состояний и не использует дополнительных запретов, диктуемых специальной теорией относительности: наличием предельной скорости и безмассовостью носителей информации (фотонов). По поводу релятивистской квантовой криптографии см., например, [17].

компонентов. Данная криптосистема по другим параметрам ни в чем не уступает наиболее развитым схемам на принципе фазового кодировании. Предлагаемый вариант может быть условно назван квантовой криптографией на временных сдвигах.

Идея криптосистемы крайне проста. В качестве носителей информации используется пара неортогональных однофотонных состояний. В каждой посылке, которая длится время $\approx 3T$, в канал связи случайно посылается одно из состояний: 0 или 1 (см. рис.1). Из-за перекрытия состояний (неортогональности, рис.1) они достоверно неразличимы. Данное обстоятельство приводит к тому, что подслушиватель принципиально не может различать состояния, распространяющиеся через канал. Неразличимость приводит к тому, что любое вторжение в канал связи будет приводить к увеличению потока ошибок на приемном конце у легитимного пользователя [3]. Легитимный пользователь на приемном конце производит измерения. Для него состояния также достоверно (с вероятностью единица) неразличимы. Если исход измерения получен от "задней" части состояния, отвечающего единице, то состояние идентифицируется однозначно. Однако вероятность такого исхода меньше единицы. Аналогично, если в канал было послано состояние, отвечающее нулю. Если фотодетектор сработал во временном окне, где имеется перекрытие состояний, то достоверное различение невозможно (так называемый inconclusive исход). После достаточно длинной серии измерений на приемном конце оставляются только те измерения, которые имели место в тех временных окнах, где состояния не перекрываются. Далее по открытому общедоступному каналу связи пользователи случайным образом раскрывают половину измерений и проверяют соответствие на приемном и передающем концах. При достаточно длинной серии измерений, как можно показать, в нераскрытых посылках вероятность ошибок такая же, как и в раскрытой. Вторжение в канал связи будет приводить к изменению статистики результатов измерений. Если вероятность ошибок в раскрытой части не превосходит некоторой критической величины, то, используя корректирующие классические коды, можно исправить ошибки в нераскрытой части, гарантируя при этом, что результирующая последовательность битов (ключ) одинакова у легитимных пользователей и неизвестна подслушивателю [14–16].

Прототип квантовой криптосистемы приведен на рис.1.

Входными состояниями является пара однофотонных состояний, сдвинутых по времени в каждой посылке (индекс поляризации опускаем как несущественный для дальнейшего):

$$|\varphi_0\rangle = \int d\hat{k}\tilde{\varphi}(\hat{k})\delta(\hat{k}^2)\theta(k_0)a^+(\hat{k})|0\rangle = \int \frac{dk}{\sqrt{k}}\frac{\tilde{\varphi}(k,k_0=|k|)}{\sqrt{k}}|k\rangle, \quad (1)$$

$$|\varphi_1\rangle = \int d\hat{k}e^{-i\hat{k}\hat{T}}\tilde{\varphi}(\hat{k})\delta(\hat{k}^2)\theta(k_0)a^+(\hat{k})|0\rangle = \int \frac{dk}{\sqrt{k}}e^{-ikT}\frac{\tilde{\varphi}(k,k_0=|k|)}{\sqrt{k}}|k\rangle, \quad (2)$$

где $\hat{k} = (k, k_0)$. Фазовый множитель e^{-ikT} описывает относительный сдвиг по времени момента приготовления состояний в разных посылках, отвечающих 0 и 1 (см. рис.1). Будем рассматривать состояния, распространяющиеся в одном направлении, именно такие состояния переносят информацию между удаленными пользователями. Обозначим $\varphi(k) \equiv \tilde{\varphi}(k, k_0 = |k|)/\sqrt{k}$. Удобно записать состояния в координатно-временном представлении. В этом представлении сдвиг по времени сводится к сдвигу аргумента в амплитуде состояния:

$$|\varphi_0\rangle = \int_{-\infty}^{\infty} d\tau\varphi(\tau)|\tau\rangle, \quad |\varphi_1\rangle = \int_{-\infty}^{\infty} d\tau\varphi(\tau - T)|\tau\rangle, \quad (3)$$

$$\varphi(\tau) = \frac{1}{2\pi}\int_0^{\infty} dke^{-ik\tau}\varphi(k), \quad |\tau\rangle = \int_0^{\infty}\frac{dk}{\sqrt{k}}e^{ik\tau}|k\rangle, \quad (4)$$

где $\tau = x - t$. Амплитуда таких состояний зависит лишь от разности $\tau = x - t$, что отражает тот факт, что если результат измерения имел место в момент t в окрестности точки $(x, x + dx)$, то такой же результат может быть получен в момент t' в окрестности точки $(x' - x + t, x' - x + t + dx)$.

Состояния (3) имеют место на выходе источника до плеча интерферометра на передающем конце (см. рис. 1). Состояния выбираются таким образом, чтобы они имели характерный масштаб локализации по времени $c \cdot l$ (далее скорость света $c = 1$), в том смысле, что в области размером l набирается почти полная нормировка (сколь угодно близкая к единице)

$$\int_l d\tau|\varphi(\tau)|^2 \approx 1. \quad (5)$$

Величина пространственно-временной локализации должна быть много меньше временной раздвижки состояний $c \cdot l \ll T$.

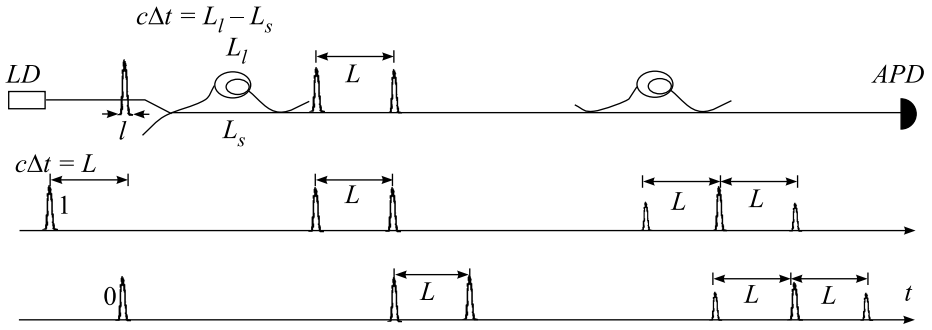

Рис.1

Сразу после источника и до входа в плечо передающего интерферометра короткие состояния не перекрываются и ортогональны. Плечо интерферометра на передающем конце представляет собой два оптоволоконных светоделителя, каждый из которых имеет один рабочий и "глухой" (вакуумный) вход и выход, а также линии задержки в одном из плеч (рис.1). Длинное плечо интерферометра на передающем конце необходимо для того, чтобы растянуть короткие входные состояния с размером $\sim l$ до более длинных, состоящих из двух "половинок" на расстоянии $L \gg l$. Причем расстояние по времени между двумя "половинками" в каждом из состояний должно быть равно временному сдвигу состояний в разных посылках (см. рис.1) для того, чтобы обеспечить перекрытие передней половинки состояния, отвечающего 1, и задней половинки, отвечающей 0. На выходе плеча интерферометра и, соответственно, на входе в линию связи состояния становятся неортогональными и достоверно неразличимыми. В канале связи на рабочем выходе состояние, отвечающее 0, имеет вид (с точностью до нормировочного множителя и общей трансляции на длину плеча)

$$|\varphi_0\rangle + |\varphi_0(T)\rangle = \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau)|\tau\rangle + \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - T)|\tau\rangle, \qquad (6)$$

где "половинка" состояния задержана на L. Соответственно для состояния, отвечающего 1, имеем

$$|\varphi_1((T)\rangle + |\varphi_1(2T)\rangle = \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - T)|\tau\rangle + \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - 2T)|\tau\rangle. \qquad (7)$$

Напомним, что временной сдвиг (T) состояний в разных посылках для 0 и 1 равен разности хода в длинном и коротком плечах интерферометра на передающем конце ($T = L = L_l - L_s$) так, что половинки перекрываются. Величина перекрытия состояний при $L \gg l$ есть $\langle\varphi_0|\varphi_1\rangle = 1/2$.

На приемном конце две "половинки" для каждого протяженного состояния сводятся вместе обратным унитарным преобразованием, которое реализуется аналогично входному. Состояние на рабочем выходе интерферометра на приемном конце, с точностью до нормировочного множителя и трансляции на длину канала связи, для 0 имеет вид

$$|\varphi_0\rangle + 2|\varphi_0(T)\rangle + |\varphi_0(2L)\rangle = \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau)|\tau\rangle + 2\int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - T)|\tau\rangle + \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - 2T)|\tau\rangle. \qquad (8)$$

И, аналогично, для состояния, отвечающего 1, имеем

$$|\varphi_1(T)\rangle + 2|\varphi_1(2T)\rangle + |\varphi_1(3T)\rangle = \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - T)|\tau\rangle + 2\int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - 2T)|\tau\rangle + \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau - 3T)|\tau\rangle. \qquad (9)$$

Происхождение трех слагаемых в формулах (8), (9) связано, грубо говоря, со следующим. Первое слагаемое, например в (8), отвечает тому, что обе "половинки" состояния прошли по длинному пути L_l, как на передающем, так и на приемном конце. Второе слагаемое возникает из-за того, что одна "половинка" прошла по длинному пути L_l на передающем и по короткому L_s на приемном концах, а вторая "половинка", наоборот, по короткому на передающем и по длинному на приемном. Третье слагаемое отвечает тому, что обе "половинки" как на приемном, так и на передающем концах прошли по короткому пути.

Обсудим теперь измерения на приемном конце. Любые измерения над однофотонными квантовыми состояниями описываются некоторым разложением единицы в одночастичном подпространстве состояний

$$I = \int\limits_0^\infty \frac{dk}{k}|k\rangle\langle k| = \int\limits_{-\infty}^{\infty} \mathcal{M}(d\tau), \qquad (10)$$

операторно-значная мера

$$\mathcal{M}(d\tau) = \frac{d\tau}{2\pi}\left(\int\limits_0^\infty \frac{dk}{\sqrt{k}} e^{-ik\tau}|k\rangle\right)\left(\int\limits_0^\infty \frac{dk'}{\sqrt{k'}} e^{ik'\tau}\langle k'|\right) \qquad (11)$$

описывает вероятность обнаружения фотона в интервале $(\tau, \tau + d\tau)$. Соответственно вероятность обнаружения фотона в конечной пространственно-временной области Ω (напомним, что амплитуда зависит лишь от разности $\tau = x - t$) есть

$$\Pr(\tau \in \Omega) = \mathrm{Tr}\{\mathcal{M}(\Omega)|\varphi\rangle\langle\varphi|\} = \\ = \int\limits_\Omega d\tau |\varphi(\tau)|^2, \quad \mathcal{M}(\Omega) = \int\limits_\Omega \mathcal{M}(d\tau). \qquad (12)$$

Пространство результатов на приемном конце состоит из трех временных областей. Первая область, накрывающая задний фронт состояния, отвечающего 1 (рис.1), есть $\Omega_1 \sim l$. Далее временное окно, накрывающее только передний фронт состояния для 0, обозначим $\Omega_0 \sim l$. Временное окно, накрывающее временную область, где состояния для 0 и 1 перекрываются, соответствует области результатов с неопределенным исходом – $\Omega_? \sim 2T$. Дополнение до всей временной оси есть $\overline{\Omega} = (-\infty, \infty)/(\Omega_0 \cup \Omega_1 \cup \Omega_?)$. Разбиение единицы выглядит следующим образом

$$I = \mathcal{M}(-\infty, \infty) = \\ = \mathcal{M}(\Omega_0) + \mathcal{M}(\Omega_1) + \mathcal{M}(\Omega_?) + \mathcal{M}(\overline{\Omega}). \qquad (13)$$

Для протокола распространения ключа важны лишь исходы во временных окнах $\Omega_{0,1}$ и $\Omega_?$. Сам по себе протокол генерации ключа представляет собой разновидность так называемого протокола BB92 [3]. Легитимный пользователь B на приемном конце оставляет лишь исходы во временных окнах Ω_0 и Ω_1, которые отвечают результату с определенным исходом (conclusive). За вероятность таких исходов отвечают операторно-значные меры $\mathcal{M}(\Omega_0)$ и $\mathcal{M}(\Omega_1)$. Данные меры аналогичны проекторам в протоколе BB92 ($\mathcal{P}_{0,1}$), которые ортогональны состояниям $|\varphi_{0,1}\rangle$ на приемном конце. Отметим, однако, что меры (11), (13) не являются проекторами из-за неортогональности базисных векторов $|\tau\rangle$.

Сам протокол с использованием измерений, описывающихся разложением (13), аналогичен исходному B92 [3] протоколу. В последнем измерение описывается проекторами $\mathcal{P}_0 = 1 - |\varphi_1\rangle\langle\varphi_1|$ и $\mathcal{P}_1 = 1 - |\varphi_0\rangle\langle\varphi_0|$. Если послано состояние $|\varphi_0\rangle$, то ненулевой исход будет в канале $\mathcal{P}_0$ с вероятностью $1 - |\langle\varphi_1|\varphi_0\rangle|^2$, и всегда будет нулевой исход на состоянии $|\varphi_1\rangle$ (вероятность такого исхода равна нулю). Аналогично, если послано состояние $|\varphi_1\rangle$, то ненулевой исход будет в канале $\mathcal{P}_1$ с вероятностью $1 - |\langle\varphi_1|\varphi_0\rangle|^2$, и всегда будет нулевой исход на состоянии $|\varphi_0\rangle$. В исходном протоколе B92 оставляются только такие ненулевые исходы. В нашем протоколе аналогом проекторов являются операторно-значные меры $\mathcal{M}(\Omega_0) \sim \mathcal{P}_1$ и $\mathcal{M}(\Omega_1) \sim \mathcal{P}_0$ (такой порядок индексов, как нам кажется, более естественный). Аналогично B92, ненулевые исходы в окне $\mathcal{M}(\Omega_0)$ имеют место только на состоянии $|\varphi_0\rangle$ и всегда равны нулю на состоянии $|\varphi_1\rangle$. И наоборот, если послано состояние $|\varphi_1\rangle$, то ненулевой исход будет только в канале $\mathcal{M}(\Omega_1)$ и никогда в канале $\mathcal{M}(\Omega_0)$. Аналогично протоколу B92, оставляются только исходы в каналах $\mathcal{M}(\Omega_{0,1})$.

В протоколе B92, кроме описанных выше, имеются также нулевые исходы в канале $\mathcal{P}_0$, если послано состояние $|\varphi_0\rangle$. Аналогично, будут также нулевые исходы в канале $\mathcal{P}_1$, когда послано состояние $|\varphi_1\rangle$, которые также отбрасываются. В нашем протоколе таким исходам с неопределенным результатом отвечают исходы, описывающиеся проекторно-значной мерой $\mathcal{M}(\Omega_?)$. Отметим, что плечо интерферометра на приемном конце принципиально для обеспечения секретности.

Далее протокол выглядит стандартным образом. После длинной серии измерений легитимные пользователи оставляют только результаты с определенным исходом. Далее случайным образом раскрывается часть исходов и оценивается вероятность ошибок. Если вероятность ошибок не превосходит некоторой критической величины (в нерелятивистских схемах предел, по-видимому, составляет $\approx 11\%$ [14–16])[3)], то далее возможна коррекция ошибок в нераскрытой части при помощи классических кодов и дальнейшее сжатие ключа (privacy amplification) для получения результирующего секретного ключа.

Приведем некоторые числовые оценки для параметров системы и краткое сравнение данной схемы с

[3)] Отметим, что в релятивистских квантовых криптосистемах предельный порог ошибок составляет 43.75% [17].

наиболее развитой схемой на принципе фазового кодирования. Главное преимущество данной схемы по сравнению с другими состоит в простоте реализации и устойчивости. В данной схеме не требуется очень точной балансировки плеч интерферометра на приемном и передающем концах. Поскольку исходно $l \ll L$, то не требуется идеально точной балансировки плеч между передающим и приемным концами интерферометра. Иначе говоря, "половинки" состояния на приемном конце не обязательно точно должны "собираться" в состояние, локализованное во временном окне l, лишь бы раздвижка за счет разной длины плеч на приемном и передающем концах не превышала L, чтобы еще можно было отличать 0 от 1 в соответствующих временных окнах. Например, если длительность входного импульса составляет $l \approx 1 \cdot 10^{-9}\,\text{с} = 1\,\text{нс}$ и раздвижка "половинок" $T \approx 10\,\text{нс}$. Данная раздвижка возникает за счет разности длин длинного и короткого путей в плече интерферометра на передающем конце, которая в пересчете на разницу путей в оптоволокне дает $L = T(c/n) \approx 200\,\text{см}$ (n – показатель преломления оптоволокна). На приемном конце для сведения двух половинок вместе требуется такая же разность длин плеч с точностью порядка длительности отдельной половинки, что составляет в пересчете на длину $l \approx 20\,\text{см}$. Это главное преимущество данной схемы по сравнению со схемой на фазовом кодировании, когда информация кодируется в разность фаз, по сути, в разность длин плеч интерферометров на передающем и приемном концах. Точность такой разности должна составлять доли длины волны, то есть разность длин плеч интерферометра на расстоянии в несколько десятков километров должна быть доли микрона, иначе схема просто не будет работать. В данной схеме достаточно точности в сантиметры.

В данной схеме на входе требуется обеспечить перекрытие половинок состояний для 0 и 1 в разных посылках (см. рис.1), чтобы состояния были неортогональны. Необходимое перекрытие половинок состояний для 0 и 1 в разных посылках может быть достигнуто, если на входе в интерферометр на передающем конце исходные "однопичковые" состояния сдвинуты по времени на величину T с точностью $\approx 1 - 2\,\text{см}$. Такой сдвиг можно реализовать при помощи дополнительного интерферометра на входе (рис.2). При этом лазер запускается тактовым генератором, работающим с постоянной скважностью $> 3T$ ($\approx 3T$ – полная длительность одной посылки). После этого импульс от лазера направляется по случайно выбранному, длинному или короткому, пути дополнительного светоделителя. Выбор пути регулируется компьютером при помощи отсекателя, который блокирует одно из плеч дополнительного интерферометра. Разность хода по разным путям равна T. При этом на выходе в разных посылках получаются как раз требуемые сдвинутые на величину T "однопичковые" состояния, которые затем растягиваются, как было описано выше. Точность длин путей, обеспечивающая перекрытие половинок состояний 0 и 1, также достаточна: порядка 1 см. При использовании дополнительного интерферометра не требуется регулировать расстояние между импульсами лазера в разных посылках и достаточно использовать обычный импульсный лазер с одной частотой следования импульсов.

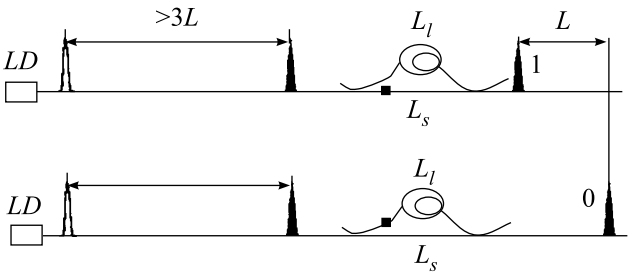

Рис.2

Выражаю благодарность М. А. Лебедеву за полезные и плодотворные обсуждения. Работа поддержана Российским фондом фундаментальных исследований (проект # 02-02-16289), проектами # 40.020.1.1.1170, # 37.029.1.1.0031, а также проектом # ДН-ЕНН-03.

1. S. Wiesner, SIGACT News, **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
4. W. K. Wootters and W. H. Zurek, Nature, **299**, 802 (1982).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).
6. H. Kosaka, A. Tomita, Y. Nambu et al., quant-ph/0306066.
7. D. Stucki, N. Gisin, O. Guinnard et al., quant-ph/0203118.
8. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993); A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995); A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).
9. Ch. Marand and P. D. Tounsend, Optics Lett. **20**, 1695 (1995); P. D. Tounsend, Nature **385**, 47 (1997); IEEE Photonics Tech. Lett. **10**,1048 (1998).

10. R. Hughes, G. G. Luther, G. L. Morgan, and C. Simmons, Lecture Notes in Computer Science **1109**, 329 (1996); R. Hughes, G. Morgan, and C. Peterson, J. Mod. Opt. **47**, 533 (2000).
11. P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995); Y. Mazurenko, R. Giust, and J. P. Goedgebuer, Optics Commun. **133**, 87 (1997).
12. F. Grosshans, G. Van Assche, J. Wenger et al., Nature **421**, 238 (2003).
13. M. Martinelli, Opt. Commun. **72**, 341 (1989); J. Mod. Opt. **39**, 451 (1992).
14. D. Mayers and A. Yao, quant-ph/9802025.
15. E. Biham, M. Boyer, P. O. Boykin et al., quant-ph/9912053.
16. P. W. Shor and J. Preskill, quant-ph/0003004.
17. С. Н. Молотков, ЖЭТФ **124**, N4(10) (2003); Письма в ЖЭТФ **78**, 194 (2003).