Письма в ЖЭТФ, том 79, вып. 10, с. 624 – 629 © 2004 г. 25 мая

О простой оценке критической длины квантового канала связи с затуханием для квантовой криптографии на когерентных состояниях

А. П. Маккавеев[+], *Д И. Помозов*[+], *С. Н. Молотков*[+*1)]

[+] *Факультет вычислительной математики и кибернетики, МГУ им. М. В.Ломоносова, 119899 Москва, Россия*

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

Поступила в редакцию 6 апреля 2004 г.

На примере протокола B92 с учетом реального затухания и сбоя фазы сигнальных когерентных состояний в одномодовом оптоволокне получена простая оценка критической длины квантового канала связи, до которой возможно секретное распространение ключа.

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. 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 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 [1, 2].

Принципиальной проблемой для секретности является затухание в квантовом канале связи. Проблема с затуханием в квантовом канале связи состоит не столько в том, что затухание, очевидно, снижает скорость передачи ключа из-за того, что не все фотоны достигают приемного конца, а в том, и это гораздо более критично, что с некоторой величины затухания *нельзя гарантировать секретность переданного ключа* [3]. Критическая величина затухания в оптоволоконных линиях связи определяется длиной канала связи. На сегодняшний день критическая длина, до которой система остается секретной, строго не известна. Оценки варьируются от 10 км до 150 км для различных квантовых криптографических протоколов [3].

Секретность передачи ключа, когда классическим битам в ключе сопоставляется пара ортогональных квантовых состояний в каждом из базисов, а состояния между базисами попарно неортогональны (протокол BB84 [4]), наиболее подробно изучена (см. работы [3, 5, 6] и ссылки в них). Секретность передачи ключа случае, когда классическим битам отвечает пара неортогональных состояний (протокол B92 [2]), менее подробно изучена, чем протокола BB84. Однако ясно, что протокол B92 менее устойчив к затуханию, чем протокол BB84, но более прост при технических реализациях и является более быстродействующим, чем протокол BB84. Из-за большей простоты протокол B92 может быть использован для передачи ключа на небольших расстояниях. Наиболее устойчивым к затуханию является, по-видимому, протокол BB84(4+2) [3], который остается секретным до длины канала связи в 150 км. Этот протокол является производным от BB84 и получается из него, если состояния для 0 и 1 внутри каждого базиса сделать неортогональными.

Нашей задачей будет получение простой оценки критической длины оптоволоконной линии связи, до которой протокол обеспечивает секретность передачи ключа.

Имеющиеся прототипы квантовых криптосистем используют, в основном, следующие принципы кодирования: 1) информация о ключе кодируется в поляризационные степени свободы [7]; 2) фазовое кодирование, когда используются несбалансированный интерферометр Маха–Цандера и информация коди-

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

руется в разность фаз, которая набирается на приемном и передающем плечах интерферометра [8–12]; 3) квантовые криптосистемы с частотной модуляцией несущей частоты [13]; 4) квантовая криптография с кодированием в непрерывные переменные (схемы на когерентных состояниях) и использованием гомодинного детектирования на приемном конце [14]. С достаточно новыми схемами на когерентных состояниях связываются определенные надежды в смысле скорости генерации ключа, однако криптографическая стойкость таких систем недостаточно исследована.

Если в квантовом канале имеется затухание, то должна существовать некоторая критическая длина канала связи, больше которой криптосистема не может гарантировать секретность ключа. Поскольку когерентные состояния являются многофотонными, то подслушиватель может при помощи светоделителя отвести часть состояния, а остальную направить через канал с меньшим затуханием или даже без затухания (что не запрещается законами природы), тем самым имитируя потери в исходном канале связи.

При извлечении секретного ключа из исходной, полученной по квантовому каналу, битовой последовательности легитимные пользователи используют процедуру коррекции ошибок и усиления секретности (privacy amplification) при помощи обмена информацией через открытый общедоступный канал связи. Такие процедуры возможны, если взаимная информация между легитимными пользователями A и B – I_{AB} – превышает взаимную информацию между подслушивателем и легитимными пользователями $I_{AB} > \max\{I_{AE,EB}\}$.

Для случая протокола распространения ключа BB84, основанного на когерентных состояниях, влияние затухания на секретность ключа исследовалось в ряде работ [15, 16]. Было высказано утверждение, что протокол на когерентных состояниях "выживает" вплоть до величины потерь в квантовом канале связи в 3 дБ [16], однако параметры квантового канала с затуханием в ответе при этом никак явно не фигурируют. Распространение квантовых состояний через канал с затуханием и дегорегентностью (сбоем фазы) приводит к искажению состояний на приемном конце даже в отсутствие подслушивателя. Подслушиватель, зная свойства исходного квантового канала связи, и то, как состояния искажаются в процессе распространения, может использовать данные обстоятельства в свою пользу. Поэтому для получения критической величины длины канала связи необходимо явно решать эволюционные уравнения для квантовых состояний в канале, что не было сделано в работах [15, 16]. В данной работе явно решаются уравнения эволюции в канале, и с учетом этого обстоятельства определяется критическая длина канала связи для стратегии подслушивания при помощи светоделителя.

Затухание в канале (поглощение фотонов и процессы декогерентности) не является унитарным преобразованием над состоянием в отличие от преобразования состояния светоделителем. Протокол прежде всего должен работать и без подслушивателя, когда состояния распространяются к приемному концу через исходный канал с затуханием, а не через замененный подслушивателем канал на более хороший с меньшим затуханием. В отсутствие подслушивателя состояние на приемном конце за счет затухания и процессов декогерентности *уже не является чистым когерентным состоянием, а представляет собой смешанное состояние.* В отсутствие подслушивателя легитимные пользователи должны извлекать секретный ключ уже из испорченных затуханием и другими процессами декогерентности смешанных состояний. Величина взаимной информации между A и B без подслушивателя должна явно зависеть от характеристик исходного квантового канала связи (констант амплитудного и фазового затухания). Легитимный пользователь A на передающем конце фиксирует сигнальные состояния, а пользователь B на приемном конце фиксирует свои измерения, последние должны быть оптимальными для различения состояний, которые получаются из чистых сигнальных когерентных состояний на передающем конце, когда они достигают приемного конца и становятся смешанными. Оптимальными в том смысле, что на данных измерениях достигается максимальная величина взаимной информации для заданных входных сигнальных состояниях и заданного квантового канала связи с затуханием и декогерентностью. Таким образом, величина взаимной информации I_{AB}, если фиксированы входные сигнальные состояния и измерения, является для всех участников протокола (легитимных и подслушивателя) априорно известной величиной. Данная величина зависит от длины квантового канала связи и является убывающей функцией длины. В пределе, когда все состояния поглощаются в канале, взаимная информация стремится к нулю, и никакая передача информации, не говоря уже о передаче секретного ключа, просто невозможна.

Критическая длина квантового канала связи, до которой еще возможно распространение секретного ключа, должна находиться из следующих соображений. Пусть сигнальные состояния на передающем конце, свойства исходного квантового канала связи,

в том числе его длина L, заданы. Это автоматически определяет оптимальные измерения для различения состояний, испорченных в исходном канале связи, и соответственно, величину взаимной информации $I_{AB}(L)$. Подслушиватель может отводить часть состояния светоделителем для своих измерений, а оставшуюся часть направлять через свой идеальный канал к пользователю B. Протокол становится не секретным, если подслушиватель различает отведенные для себя состояния с меньшей вероятностью ошибки, чем пользователь B различает состояния, доставленные ему подслушивателем через идеальный канал, при помощи своих измерений, которые являются оптимальными для исходных испорченных состояний, но не являются таковыми для состояний от подслушивателя.

Обнаружение подслушивателя происходит путем раскрытия легитимными пользователями через открытый классический канал, случайным образом выбранной, примерно половины переданной последовательности. Для нее вычисляется $\overline{I}_{AB}$, если данная величина $\overline{I}_{AB}(L) < I_{AB}(L)$, то протокол обрывается.

Далее, секретная передача ключа невозможна, если найдется хотя бы одна атака подслушивателя на ключ, при которой

$$I_{AB}(L) < \max_{\text{all attacks}} \{I_{AE}\}. \tag{1}$$

Соответственно, протокол будет обеспечивать секретность ключа, если для любых атак на ключ

$$I_{AB}(L) > \max_{\text{all attacks}} \{I_{AE}\}. \tag{2}$$

Достаточно сравнивать только I_{AE} с I_{AB}, поскольку $I_{BE} < I_{AE}$.

Поскольку сигнальные состояния и измерения раз и навсегда фиксированы в начале протокола, *независимо от присутствия подслушивателя*, *и физические свойства исходного квантового канала известны*, то неравенство (2) будет определять критическую длину квантового канала связи, до которой возможно секретное распространение ключа. Верхняя оценка на длину канала связи имеет место, если в качестве $I_{AB}(L)$ берется пропускная способность *исходного* квантового канала связи.

Наибольшую трудность составляет перебор всевозможных атак на ключ подслушивателем. На сегодняшний день исчерпывающее доказательство секретности протокола B92 в канале с затуханием отсутствует.

Ниже на примере протокола B92, использующего пару неортогональных когерентных состояний, нами будет явно введено затухание и фазовая декогерентность в квантовом канале связи и рассмотрена устойчивость протокола относительно конкретной атаки при помощи светоделителя, когда часть состояния отводится подслушивателем.

Сигнальные состояния. В качестве сигнальных состояний выберем пару неортогональных когерентных состояний, которые возникают на выходе одномодового лазера. Соответственно, $0 - |+\alpha\rangle$ и $1 - |-\alpha\rangle$:

$$|\pm\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{(\pm\alpha)^n}{\sqrt{n!}} |n\rangle, \tag{3}$$

где $(a^+)^n|0\rangle = |n\rangle$ – n-частичное фоковское состояние, a^+ – оператор рождения, $|0\rangle$ – вакуумное состояние, описывающее пустой канал связи. Входная матрица плотности имеет вид

$$\rho = \frac{1}{2}(\rho_+ + \rho_-), \quad \rho_\pm = |\pm\alpha\rangle\langle\pm\alpha|. \tag{4}$$

Исходный квантовый канал связи с затуханием и декогерентностью. Физические свойства квантового канала связи описываются двумя константами – амплитудным затуханием и фазовым. Эволюция матрицы плотности в канале описывается стандартным уравнением

$$\frac{d}{d\tau}\rho = \Gamma_a\left(a\cdot\rho\cdot a^+ - \frac{1}{2}a^+a\cdot\rho - \frac{1}{2}\rho\cdot a^+a\right) + \\ + \Gamma_p\left(a^+a\cdot\rho\cdot a^+a - \frac{1}{2}(a^+a)^2\cdot\rho - \frac{1}{2}\rho\cdot(a^+a)^2\right), \tag{5}$$

где Γ_a и Γ_p – константы амплитудного и фазового затухания на единицу длины, $\tau = x - ct$. Константа амплитудного затухания Γ_a для оптоволокна известна достаточно точно, например, для длины волны 1550 нм, на которой достигается минимум затухания в одномодовом оптоволокне, величина $\Gamma_a = 0.17 - 0.25$ дБ/км в зависимости от типа одномодового оптоволокна.

Амплитудное затухание ответственно за поглощение фотонов в канале связи и приводит к экспоненциальному уменьшению среднего числа фотонов в зависимости от длины. При $\Gamma_p = 0$ имеем

$$\frac{d}{d\tau}\langle n\rangle = \mathrm{Tr}\{a^+a\frac{d}{d\tau}\rho\} = -\tilde{\Gamma}_a\langle n\rangle, \\ \langle n(\tau)\rangle = 10^{-\Gamma_a\tau/10}\langle n(0)\rangle. \tag{6}$$

Фазовая декогерентность сохраняет число частиц и приводит к затуханию недиагональных компонент матрицы плотности. При $\Gamma_a = 0$ имеем

$$\frac{d}{d\tau}\rho_{nm} = \Gamma_p(n\cdot m - \frac{1}{2}n^2 - \frac{1}{2}m^2)\rho_{nm} = \\ = -\frac{\Gamma_p}{2}(n-m)^2\rho_{nm}, \quad \rho_{nm} = \langle n|\rho|m\rangle. \qquad (7)$$

Эволюция недиагональных компонент матрицы плотности имеет вид

$$\rho_{nm}(\tau) = \rho_{nm}(0)e^{[-\frac{1}{2}\Gamma_p\tau(n-m)^2]}. \qquad (8)$$

В общем случае уравнение движения для матрицы плотности не может быть решено аналитически, поэтому приходится прибегать к численным методам.

Измерения на приемном конце. Пусть длина канала фиксирована и равна L. Матрица плотности на приемном конце определяется как решение уравнения движения (5) при начальных условиях (4). Обозначим матрицу плотности на выходе квантового канала связи как $\rho(L)_{\pm}$. Протокол должен работать прежде всего в отсутствие подслушивателя. Будем считать, что легитимный пользователь ограничен на приемном конце лишь индивидуальными измерениями над состояниями в каждой посылке, поскольку их технически проще реализовать. Оптимальное измерение, которое минимизирует ошибку при различении пары состояний $\rho_-(L)$ и $\rho_+(L)$ с одинаковыми априорными вероятностями на выходе $\pi_- = \pi_+ = 1/2$, известно [17,18]. Такое измерение дается разложением единицы

$$I = \mathcal{M}_+ + \mathcal{M}_-. \qquad (9)$$

Оператор $\mathcal{M}_-$ является проектором на собственное подпространство оператора $\frac{1}{2}(\rho_+(L) - \rho_-(L))$. Минимальная вероятность ошибки при этом равна

$$p_e(L) = \frac{1}{2}\left(1 - \|\frac{1}{2}\left(\rho_+(L) - \rho_-(L)\right)\|_+\right), \qquad (10)$$

где норма определяется как $\|T\|_1 = \mathrm{Tr}|T|$ – следовая норма оператора T, и $|T| = T_+ + T_-$, соответственно, $T_+(T_-)$ положительная (отрицательная) часть эрмитова оператора. Норма в (10) определяется как сумма положительных собственных чисел оператора.

Взаимная информация между A и B при таком способе измерения равна [18]

$$I_{AB}(L) = 1 - h(p_e(L)), \\ h(x) = x\log x + (1-x)\log(1-x). \qquad (11)$$

и совпадает с так называемой классической пропускной способностью квантового канала связи за один шаг (one shot)[18]. Грубо говоря, данная величина есть классическая информация в битах в пересчете на одну посылку, которая при использовании оптимальных измерений (9) может передана от A к B безошибочно (точнее, со сколь угодно малой вероятностью ошибки) при достаточно длинной последовательности.

Если легитимные пользователи не ограничены индивидуальными измерениями, а могут выполнять измерения над целыми достаточно длинными блоками передаваемых состояний, то максимальная достижимая величина взаимной информации ограничена классической пропускной способностью квантового канала связи [18], которая определяется как

$$C(L) = H\left(\frac{1}{2}\rho_+(L) + \frac{1}{2}\rho_-(L)\right) - \frac{1}{2}H(\rho_+(L)) - \\ - \frac{1}{2}H(\rho_-(L)), \quad H(\rho) = -\mathrm{Tr}\{\rho\log\rho\}. \qquad (12)$$

Протокол генерации секретного ключа. Проводится длинная серия посылок и измерений. В итоге легитимные участники A и B имеют, вообще говоря, различные строки бит. Случайной выборкой через открытый канал связи легитимные пользователи раскрывают примерно половину бит, производят их сравнение и оценивают вероятность несовпадений (вероятность ошибки). При достаточно длинной последовательности вероятность того, что ошибка в нераскрытой части последовательности такая же, как в раскрытой, стремится к единице. Вероятность ошибки дает величину взаимной информации между A и B. Если полученная величина совпадает с априорной оценкой (11), то протокол продолжается. В противном случае протокол прерывается.

Подслушивание при помощи "расщепления" состояний светоделителем. Рассмотрим теперь устойчивость протокола относительно стратегии подслушивания, когда часть состояния "расщепляется" светоделителем. Более конкретно, подслушиватель, находясь вблизи передающего узла A, отводит часть состояния светоделителем, а остальную направляет к участнику B через свой канал без затухания.

Нашей задачей будет оценка исходной длины (L) квантового канала связи с затуханием при которой подслушиватель не сможет иметь большую взаимную информацию $I_{AE}(\eta)$, чем легитимные пользователи ($I_{AE}(\eta) < I_{AB}(\eta)$), оставаясь при этом незамеченным. Коэффициент светоделителя η подслушиватель может выбирать по своему усмотрению. При заданной длине исходного канала связи L протокол будет обеспечивать передачу секретного ключа до тех пор, пока выполняется неравенство $I_{AE}(\eta) < I_{AB}(\eta) = I_{AB}(L)$. Критическая длина канала связи будет определяться из условия $I_{AE}(\eta) =$

Среднее число фотонов $\mu = \|\alpha\|^2$	Амплитудное затухание Γ_a	Фазовое затухание Γ_p	Критическая длина канала связи L (км)
0.1	0.2	0.01	14.3
0.3	0.2	0.01	14.1
1.0	0.2	0.01	13.4
3.0	0.2	0.01	11.5
0.1	0.2	0.05	11.8
0.3	0.2	0.05	11.2
1.0	0.2	0.05	9.4
3.0	0.2	0.05	7.6
0.1	0.2	0.01	9.4
0.3	0.2	0.01	9.4
1.0	0.2	0.01	8.4
3.0	0.2	0.01	7.1

$I_{AB}(\eta) = I_{AB}(L)$. Это дает также величину коэффициента светоделителя η_c. Подслушиватель не может выбрать (при данной длине канала) бóльшую величину η, в противном случае его присутствие обнаруживается легитимными пользователями, при этом $I_{AE}(\eta > \eta_c) > I_{AB}(\eta)$.

Исходные когерентные состояния факторизуются в тензорное произведение состояний $|\pm\alpha\rangle \to |\pm\sqrt{\eta}\alpha\rangle \otimes |\pm\sqrt{1-\eta}\alpha\rangle$ и являются независимыми, поэтому измерения подслушивателя и легитимного пользователя над своими состояниями не влияют друг на друга. На приемном конце легитимный пользователь проводит измерения, описывающиеся разложением единицы (9), над состояниями $|\pm\sqrt{1-\eta}\alpha\rangle$, которые доставляет подслушиватель через свой идеальный канал связи. Возникающая при этом взаимная информация есть $I_{AB}(\eta)$.

При данной атаке на передаваемый ключ подслушиватель остается незамеченным до тех пор, пока

$$I_{AE}(\eta) \le I_{AB}(L) = I_{AE}(\eta). \tag{13}$$

При фиксированном коэффициенте светоделителя η величина взаимной информации $I_{AE}(\eta)$ не может превосходить величины классической пропускной способности идеального квантовго канала связи с входными состояниями $|\pm\sqrt{\eta}\alpha\rangle$ с априорными вероятностями, равными $1/2$. Последняя равна [18]:

$$C_{AE}(\eta) = -\left(\frac{1-\varepsilon}{2}\right)\log\left(\frac{1-\varepsilon}{2}\right) - \left(\frac{1+\varepsilon}{2}\right)\log\left(\frac{1+\varepsilon}{2}\right), \tag{14}$$

$$\varepsilon = \langle\sqrt{\eta}\alpha| - \sqrt{\eta}\alpha\rangle = \mathrm{e}^{-\eta|\alpha|^2/2}.$$

Если подслушиватель ограничивается лишь индивидуальными измерениями, то величина взаимной информации $I_{AE}(\eta)$ не может превосходить величины классической пропускной способности канала между ним и пользователем A за один шаг [18]

$$C_{AE}^{(1)}(\eta) = \frac{1}{2}\left[(1+\sqrt{1-\varepsilon^2})\log(1+\sqrt{1-\varepsilon^2}) + (1-\sqrt{1-\varepsilon^2})\log(1-\sqrt{1-\varepsilon^2})\right]. \tag{15}$$

Численная процедура. Уравнения эволюции (5) решались численными методами. Длина канала связи разбивалась на дискретные интервалы с шагом Δl. Матрица плотности в базисе чисел заполнения заменялась матрицей конечного размера $N \times N$ ($\rho_{nm} = 0$ при $n, m > N$). Анализ численной процедуры дает, что величина разбиения не должна превосходить $\Delta l < 1/\Gamma_a \cdot N$. Для проверки процедуры на каждом шаге вычислялось среднее число частиц $\sum_n \rho_{nn} n$, для которого имеется точное решение (6) в отсутствие фазовой декогерентности.

Критическая длина. Критическая длина канала, до которой система допускает распространение секретного ключа, приведены в таблице для различных значений константы фазового затухания Γ_p. Значение константы амплитудного затухания равно Γ_a, что отвечает величине минимального затухания в одномодовом оптоволокне при длине волны 1550 нм. В двух верхних частях таблицы показаны значения длины для случая, когда подслушивателем используются индивидуальные оптимальные измерения (15). В нижней трети – значения критической длины, когда подслушиватель использует коллективные измерения (14). Данные простые оценки хорошо согласуются с результатами [5], полученных другим методом. *Отметим, что данную оценку не следует переносить на другие квантовые протоколы распространения секретного ключа.* Оценки длины для протокола BB84 для однофотонных состояний (точнее, квазиоднофо-

тонных, когда $\mu = 0.1$) дают ~ 50 км, а для наиболее устойчивого к затуханию протокола BB84(4+2) составляют ~ 150 км. Данные ограничения по затуханию (по длине канала связи) связаны фактически с тем, что секретность основана лишь на геометрических свойствах векторов состояний в гильбертовом пространстве. Отметим, что в системах релятивистской квантовой криптографии, секретность которых базируется на ограничениях не только квантовой механики, но и специальной теории относительности (на принципе релятивистской причинности), секретность сохраняется при любом уровне затухания [19]. Затухание уменьшает лишь скорость распространения ключа.

Работа поддержана Российским фондом фундаментальных исследований (проект # 02-02-16289).

1. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. A. Acin, N. Gisin, and V. Scarani, quant-ph/0302037.
4. C. H. Bennett and G.Brassard, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
5. N. Lutkenhaus, Phys. Rev. **A61**, 052304 (2000).
6. K. Tamaki, M. Koashi, and N. Imoto, quant-ph, 0212161 (2002).
7. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).
8. H. Kosaka, A. Tomita, Y. Nambu et al., quant-ph/0306066.
9. D. Stucki, N. Gisin, O. Guinnard et al., quant-ph/0203118.
10. 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).
11. 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).
12. 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).
13. 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).
14. F. Grosshans, G. Van Assche, J. Wenger et al., Nature **421**, 238 (2003).
15. F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
16. Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
17. C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, (1976).
18. А. С. Холево, Проблемы передачи информации **15**, 3 (1979); Успехи математических наук. **53**, 193 (1998); *Введение в квантовую теорию информации*, серия *Современная математическая физика, вып.5*, МЦНМО, Москва, 2002.
19. С. Н. Молотков, *Многофотонная квантовая криптография для свободного пространства: о передаче секретных ключей на спутники*, ЖЭТФ (в печати).