Письма в ЖЭТФ, том 78, вып. 3, с. 194 – 200 © 2003 г. 10 августа

Простая схема квантовой криптографии на задержках на базе оптоволоконного интерферометра Маха-Цандера

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
119899 Москва, Россия

Поступила в редакцию 10 июня 2003 г.

После переработки 1 июля 2003 г.

Предложена простая экспериментальная схема релятивистской квантовой криптосистемы на базе оптоволоконного интерферометра Маха–Цандера, в которой детектирование любых попыток подслушивания гарантируется законами квантовой механики и ограничениями, диктуемыми специальной теорией относительности.

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

К настоящему времени существует достаточно большое число предложений и экспериментальных реализаций схем для квантовой криптографии [1]. Практически все схемы для обеспечения секретного распространения ключа используют два запрета, диктуемых квантовой механикой. Запрет на копирование неизвестного квантового состояния (no cloning-теорема [2]), и запрет на различение квантовых состояний без их возмущения, если они являются неортогональными [3]. Эти два, тесно связанных между собой, запрета позволяют детектировать любые попытки подслушивания и обеспечивать безусловную секретность. В нерелятивистской квантовой механике для ортогональных состояний нет запретов на копирование и различение без их возмущения [2, 3]. Как было показано ранее [4 – 6], теоретический предел для допустимых ошибок на приемном конце, до которого еще можно гарантировать секретность ключа, например, для протокола BB84, составляет 11% [4, 6]. Этот предел фактически возникает из-за того, что невозможно отличить ошибки из-за шума в канале от ошибок, которые вызваны подслушивателем, поэтому для того, чтобы гарантировать секретность ключа, неизбежно приходиться считать, что все ошибки вызваны действиями подслушивателя.

Упомянутые схемы никак явно не используют того факта, что единственными приемлемыми носителями информации на большие расстояния являются фотоны (состояния безмассового квантованного электромагнитного поля). То обстоятельство, что квантованное безмассовое поле фотонов распространяется в вакууме с предельно допустимой скоростью, позволяет использовать ограничения, диктуемые специальной теорией относительности для обеспечения секретного распространения ключа в квантовой криптографии. Причем секретность ключа достигается даже при использовании ортогональных состояний. Ранее были предложены релятивистские схемы квантовой криптографии на ортогональных состояниях фотонного поля [7,8]. Протоколы обмена в [7,8] используют ортогональные состояния с протяженностью, превышающей длину канала связи. Последнее принципиально достижимо, однако трудно реализуемо экспериментально. Недавно было показано, что для секретного распространения ключа с учетом ограничений, накладываемых как квантовой природой состояний, так и специальной теорией относительности, можно использовать однофотонные состояния с любой протяженностью, в том числе и с протяженностью, меньшей длины канала связи [9]. Кроме того, теоретический предел ошибок на приемном конце, до которого еще можно гарантировать секретность ключа, составляет $43.75\% = 7/16$, что заметно превышает допустимый порог ошибок для нерелятивистских схем. Последнее связано с тем, что удается частично разделить ошибки, вызываемые подслушивателем и шумом в канале.

Ниже предлагается простая реализация квантовой криптосистемы на базе оптоволоконного интерферометра Маха–Цандера. Причем, в отличие от предыдущих схем, данная схема не требует поляризационного контроля и “идеальной” балансировки плеч интерферометра на передающем и приемном концах. Кроме

[1)] Основной адрес: 142132 Черноголовка, Московская обл., ИФТТ РАН

того, допустимая вероятность ошибки на приемном конце составляет $\approx 25\%$, что хотя и ниже теоретического предела для релятивистских схем [9], но все же вдвое выше, чем для нерелятивистских схем на базе аналогичных интерферометров. Последнее связано с тем, что ограничения квантовой механики вместе со специальной теорией относительности оказываются *боле жесткими, чем просто ограничения квантовой механики.

Невозможность копирования произвольных квантовых состояний $|\varphi_0\rangle$ и $|\varphi_1\rangle$ означает, что невозможен процесс [2]

$$|\varphi_0\rangle \mapsto |\varphi_0\rangle|\varphi_0\rangle, \quad |\varphi_1\rangle \mapsto |\varphi_1\rangle|\varphi_1\rangle. \tag{1}$$

Для ортогональных состояний такой запрет в квантовой механике отсутствует [2]. Невозможность получения информации об одном из квантовых состояний $|\varphi_0\rangle$ и $|\varphi_1\rangle$ без их возмущения означает невозможность процесса [3]

$$\begin{aligned} U(|\varphi_0\rangle|A\rangle) &\mapsto |\varphi_0\rangle|A_0\rangle, \\ U(|\varphi_1\rangle|A\rangle) &\mapsto |\varphi_1\rangle|A_1\rangle, \quad |A_0\rangle \neq |A_1\rangle, \end{aligned} \tag{2}$$

если состояния неортогональны, $\langle\varphi_0|\varphi_1\rangle \neq 0$. Для ортогональных состояний нет запрета на достоверное различение без их возмущения [3], точнее говоря, теорема [3] в этом случае ничего не говорит. Часто произносимые слова при интерпретации данной теоремы о том, что ортогональное состояние "проходит" через вспомогательную систему $|A\rangle$, взаимодействует по мере прохождения с ней, и изменяет ее состояние, не соответствуют содержанию теоремы. В теореме ничего подобного нет, в том смысле, что она носит чисто геометрический характер и утверждает, что вектор состояния вспомогательной системы $|A\rangle$ может быть унитарно повернут в зависимости от входного вектора $|\varphi_{0,1}\rangle$ и переведен в новое состояние $|A_0\rangle$ или $|A_1\rangle$ без изменения входного вектора. При этом неявно предполагается, что входной вектор $|\varphi_{0,1}\rangle$ доступен как целостный объект, то есть для совершения унитарного преобразования U нужно иметь доступ ко всему пространству состояний $\mathcal{H}_{\varphi_{0,1}}$, где отличен от нуля носитель состояния, в противном случае преобразование не будет унитарным. Тот факт, что в доказательстве фигурирует лишь вектор состояния как целостный объект $|\varphi_{0,1}\rangle$ без внутренней координатной "начинки", как раз и подразумевает, что вектор состояния при унитарном преобразовании участвует "сразу целиком".

Для любой реальной физической системы гильбертово пространство $\mathcal{H}_{\varphi_{0,1}}$ неизбежно привязано к пространству-времени Минковского, где состояние имеет амплитуду (сглаживающую волновую функцию). Доступ к гильбертову пространству состояний неизбежно подразумевает доступ к той части пространства-времени, где отлична от нуля амплитуда (волновая функция) состояния. Если же доступна лишь часть пространства, где отлична от нуля амплитуда состояний, то в этом случае даже ортогональные состояния невозможно достоверно скопировать или различить. Последнее более менее очевидно, поскольку никакой процесс, в том числе копирование или различение, не может иметь вероятность исхода больше, чем доля нормировки состояний, которая набирается в доступной пространственно-временной области, и тем самым автоматически в доступной части гильбертова пространства. Грубо говоря, чтобы с достоверностью скопировать или различить ортогональные состояния, они нужны сразу и целиком.

Поэтому, если амплитуда состояния отлична от нуля в некоторой конечной области пространства-времени, то слова о том, что состояние доступно целиком, означают доступ к этой области. В нерелятивистской квантовой механике, где нет ограничений на предельную скорость, доступ к любой конечной области может быть получен мгновенно. В квантовой теории поля, где существуют ограничения на предельную скорость, доступ к состоянию целиком может быть получен лишь в том случае, если протяженное состояние предварительно унитарно преобразовано к состоянию с амплитудой, отличной от нуля лишь в сколь угодно малой пространственной области. После этого можно пользоваться теоремой [2, 3]. Из-за принципа релятивистской причинности [10] такое унитарное преобразование состояния, заданного в конечной пространственно-временной области, в состояние, локализованное в сколь угодно малой пространственной области, может быть осуществлено лишь за конечное время. Минимально необходимое время определяется из условия накрытия прошлой частью светового конуса исходной пространственной области, где была отлична амплитуда состояния (см. рис.1). Вершина этого конуса находится в сколь угодно сильно локализованной области (точке), в которую унитарно преобразуется исходная амплитуда состояния. Каждое из пары ортогональных состояний, унитарно преобразованных ("собранных") в локализованной области, может быть после этого достоверно скопировано или различимо. Поскольку речь идет о безмассовых состояниях квантованного поля (фотонов), которые распространяются с предельно допустимой скоростью, то такое унитарное преобразование и дальнейшее копирование приведет к сдвигу (задержке) состояний в пространстве-времени по сравнению с исходной свободной эволю-

цией (распространением) состояний. Данное обстоятельство позволяет детектировать любые попытки подслушивания. Отметим, что ограничения, накладываемые на измерения в релятивистской области, исследовались в работе [11], а затем были продолжены в [12].

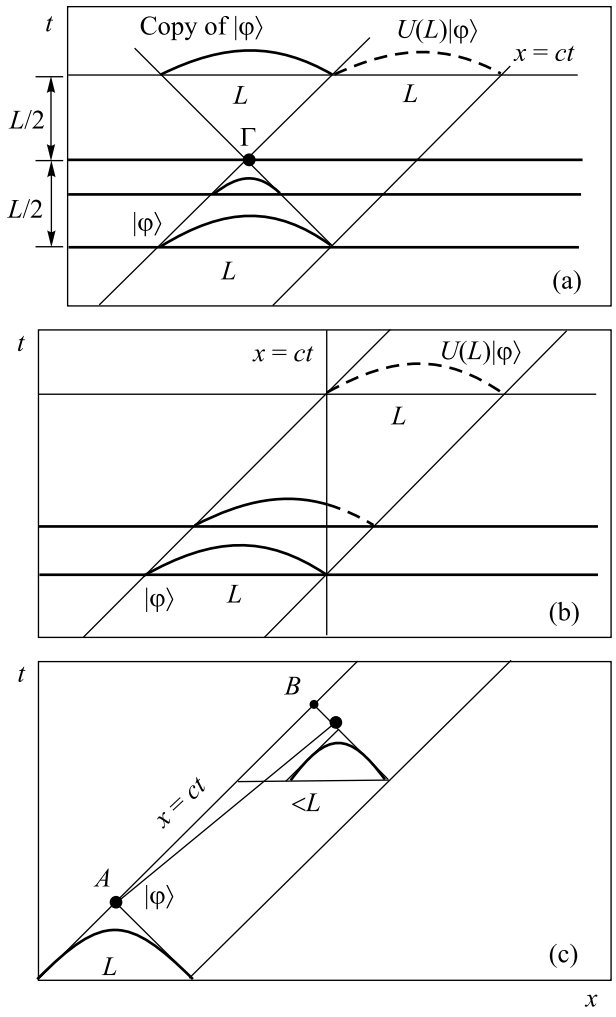

Рис.1

Иначе говоря, для ортогональных состояний безмассового квантованного поля теорема о запрете копирования звучит следующим образом. Ортогональные состояния могут быть с вероятностью сколь угодно близкой к единице скопированы. Но при этом в результате копирования получаются состояния с той же формой амплитуд, но сдвинутые (транслированные в пространстве-времени). То есть разрешен более слабый процесс по сравнению с нерелятивистским случаем в (1):

$$|\varphi_0\rangle \mapsto (U_L|\varphi_0\rangle)(U_L|\varphi_0\rangle), \quad |\varphi_1\rangle \mapsto (U_L|\varphi_1\rangle)(U_L|\varphi_1\rangle). \tag{3}$$

Здесь U_L – оператор трансляции в пространстве-времени вдоль ветви светового конуса величины $L = \Delta(x-t)$ – размера области, где отлична от нуля амплитуда состояний (считаем, для краткости, что оба состояния отличны от нуля в одинаковой пространственно-временной области, но отличаются формой амплитуд $\varphi_{0,1}(x-t)$).

Аналогично модифицируется теорема [3] при различении ортогональных состояний, разрешен лишь более слабый процесс по сравнению с нерелятивистским случаем (2):

$$\begin{gathered} |\varphi_0\rangle|A\rangle \mapsto (U_L|\varphi_0\rangle)|A_0\rangle, \\ |\varphi_1\rangle|A\rangle \mapsto (U_L|\varphi_1\rangle)|A_1\rangle, \quad |A_0\rangle \neq |A_1\rangle. \end{gathered} \tag{4}$$

Сказанное удобно пояснить при помощи диаграмм рис.1a,b.

Поскольку амплитуда состояний безмассового квантованного поля, распространяющихся в одном направлении оси x, зависит лишь от разности $x-t$, то можно провести рассуждения, фиксируя время и считая переменной координату, либо наоборот. Сделаем это для обоих случаев. Этими двумя случаями исчерпываются все ситуации. Пусть задано одно из ортогональных состояний с амплитудой $\varphi(x-t)$, распространяющихся со скоростью света ($c=1$, индекс состояния 0 или 1 для краткости пока опустим). Пусть состояние сосредоточено в области L в том смысле, что $\int_L |\varphi(x-t_0)|^2 dx \approx 1, \varphi_{0,1}(x-t_0)$ – амплитуда на временном срезе t_0.

Чтобы иметь *сразу все значения амплитуды состояния при всех x в момент t_0* в той области, где она отлична от нуля, необходимо совершить унитарное преобразование сразу над всем состоянием. Пусть унитарное преобразование над амплитудой состояния – $U\varphi_{0,1}(x-t_0) = \tilde{\varphi}_{0,1}(x'-t)$ $(t > t_0)$, амплитуда нового состояния $\tilde{\varphi}(x'-t)$ может быть отлична от нуля уже в меньшей пространственной области. Минимальный размер области по x' к моменту t диктуется релятивистским принципом причинности [10]. Матричные элементы унитарного оператора отличны от нуля только тогда, когда точки (x,t_0) и (x',t) лежат внутри прошлой части светового конуса, выпущенного из точки Г, и накрывающей область, где отлична от нуля амплитуда состояния в момент t_0. К моменту, не ранее, чем амплитуда исходного состояния L может быть унитарным образом преобразована в состояние со сколь угодно сильно локализованной амплитудой в окрестности Г. Принципиально важно, что это будет уже *другое* состояние, чем исходное $\varphi(x-t_0)$. К моменту Г доступны значения амплитуды состояния при всех x сразу (мгновенно). Теперь можно мгновенно получить исход измерения и иметь

полную (с вероятностью единица) информацию о состоянии. Если пара исходных состояний была ортогональна, то можно унитарным преобразованием получить также пару ортогональных состояний к моменту Г и, соответственно, достоверно отличить одно от другого (теперь уже можно воспользоваться теоремой [2] о достоверной различимости ортогональных состояний). Подчеркнем еще раз, что это будут уже *другие* ортогональные состояния, отличные от исходных. "Восстановление" или копирование состояния также может быть реализовано обратным унитарным преобразованием, "направленным" вперед во времени. Состояние с той же формой амплитуды как исходное может быть получено к моменту не ранее, чем это диктуется релятивистской причинностью. Амплитуда состояния, с той же формой как у исходного, находится в передней части светового конуса, выпущенного из точки Г. Полученное состояние также *другое* по сравнению с исходным, в том смысле, что оно запаздывает по времени, по отношению к исходному состоянию, которое успело бы распространиться вперед по x к моменту L, как раз на величину L, если бы не было попыток копирования или получения информации о нем (рис.1a)). Пока речь шла о получении информации о состояниях в канале с вероятностью единица. Те же самые рассуждения годятся для получения информации с вероятностью, меньшей единицы. Задержка при этом будет меньше L (рис.1a,b).

Рассуждения работают и в нерелятивистском случае. Если игнорировать ограничения специальной теории относительности, то из предыдущего рассмотрения нужно выбросить ту часть, которая аппелирует к световому конусу. При этом унитарные преобразования можно делать формально мгновенно, и из рассмотрения даже можно исключить явное присутствие координаты, оставив неявно только то, что при унитарном преобразовании состояния доступны целиком (целиком мгновенно доступно вся пространственная область).

Аналогично можно провести рассуждения, когда состояние унитарным образом преобразуется в состояние вспомогательной локализованной системы. Пример такого унитарного преобразования имеет место при "остановке" света [13]. Данное унитарное преобразование переводит состояние фотонного поля в вакуумное состояние из-за его безмассовости и невозможности иметь нулевую скорость распространения, а состояние атомной системы – в некоторое новое состояние. Преобразование, будучи унитарным, также требует доступа ко всем значениям амплитуды фотонного пакета в точке локализации атомной системы. Такой доступ достигается естественным образом по мере распространения пакета со скоростью света и достижения им локализованной атомной системы ("вхождение" пакета целиком в атомную систему). Данный процесс, если речь идет о получении результата с вероятностью единица, также требует времени L (однофотонный пакет должен целиком "войти" в атомную систему). При этом фотонное поле оказывается в *другом – вакуумном состоянии*, а вспомогательная система – в новом состоянии в зависимости от входного фотонного состояния. К моменту времени L с вероятностью единица можно выяснить, что это за состояние и приготовить такое же, но с неизбежной задержкой на L, которая будет иметь место по сравнению со свободным распространением исходного пакета (рис.1b).

Для дальнейшего также важно, что никакая эволюция безмассового квантованного поля, взаимодействующего с окружением (другими квантовыми и классическими степенями свободы в канале), не может привести к "сжатию" состояния в том смысле, что нормировка состояния будет набираться в меньшей пространственной области, выходящей за световой конус, по сравнению со свободным распространением (см. рис.1c)). Как правило, такое взаимодействие приведет к тому, что состояние будет смешанным, но носитель матрицы плотности в пространстве-времени не может быть "сжат" и выведен за световой конус (рис.1c). В противном случае это бы давало возможность передавать информацию при помощи квантовых состояний быстрее скорости света. Действительно, пусть имеется одно из пары ортогональных квантовых состояний (рис.1c). Участник A может извлечь классическую информацию из квантового состояния не ранее, чем в момент времени, определяемый условием накрытия амплитуды состояния прошлой частью светового конуса. После этого он может передать уже классическую информацию к участнику B. Такая передача не может быть сделана быстрее, чем скоростью света (наблюдатели соединены ветвью светового конуса, рис.1c). Если бы в результате эволюции квантового состояния в канале оно могло "сжаться" таким образом, чтобы при накрытии состояния прошлой частью светового конуса вершина этого конуса оказывалась в пространственно-подобной области по отношению к световому конусу с вершиной в точке A, одна из ветвей которого проходит через точку B. В этом случае наблюдатель B мог бы извлечь классическую информацию из квантового состояния раньше, чем ее мог бы передать со скоростью света участник A, поскольку вершина светового конуса, накры-

вающего "сжатое" квантовое состояние, выходит в пространственно-подобную область.

Для криптографии сказанное означает, что шум в канале не дает подслушивателю ни скопировать, ни получить информацию о состоянии раньше, чем это диктуется диаграммами на рис.1a,b (величина ошибки подслушивателя при условии прохождения временного теста на задержку не может быть меньше, чем (12), см.ниже).

Перейдем к описанию криптосистемы на базе оптоволоконного интерферометра (рис.2). Входными состояниями является пара ортогональных однофо-

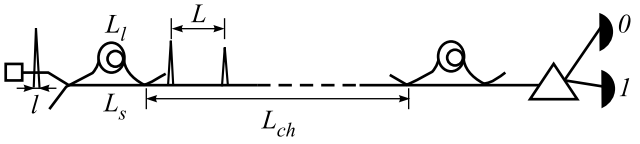

Рис.2

тонных состояний следующего вида (индекс поляризации опускаем как несущественный для дальнейшего):

$$|\varphi_{0,1}\rangle = \int_{\Delta k_{0,1}} d\hat{k}\tilde{\varphi}_{0,1}\delta(\hat{k}^2)\theta(k_0)a^+(\hat{k})|0\rangle = \\ = \int_{\Delta k_{0,1}} \frac{dk}{\sqrt{k}}\frac{\tilde{\varphi}(k,k_0=|k|)}{\sqrt{k}}|k\rangle, \qquad (5)$$

где $\hat{k} = (k, k_0)$, состояния заданы в неперекрывающихся частотных интервалах $\Delta k_{0,1}$, которые далее будем считать для краткости одинаковыми. Будем рассматривать состояния, распространяющиеся в одном направлении, именно такие состояния переносят информацию между удаленными пользователями. Обозначим $\varphi_{0,1}(k) \equiv \tilde{\varphi}(k, k_0 = |k|)/\sqrt{k}$. Удобно записать состояния в координатно-временном представлении

$$|\varphi_{0,1}\rangle = \int_{-\infty}^{\infty} d\tau\varphi_{0,1}(\tau)|\tau\rangle, \qquad (6)$$

$$\varphi_{0,1}(\tau) = \int_{\Delta k} dk\mathrm{e}^{-ik\tau}\varphi(k), \quad |\tau\rangle = \int_{\Delta k}\frac{dk}{\sqrt{k}}\mathrm{e}^{ik\tau}|k\rangle, \qquad (7)$$

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 $(x', x' - x + t + dx)$. Далее для краткости будем говорить, что амплитуды $\varphi_{0,1}(\tau)$ заданы на ветви светового конуса.

Состояния выбираются достаточно локализованными, в том смысле, что в области размером l набирается почти полная нормировка (сколь угодно близкая к единице)

$$\int_l d\tau|\varphi_{0,1}(\tau)|^2 \approx 1. \qquad (8)$$

Величина пространственно-временной локализации определяется величиной Δk и $l \approx 1/\Delta k$ (более точные соотношения см. в [9]).

Перейдем к описанию протокола. Участник A случайным образом в каждой посылке выбирает одно из состояний $|\varphi_0\rangle$ или $|\varphi_1\rangle$ в заранее всем известные моменты времени. Предполагается, что длина канала связи известна заранее и часы на обоих концах синхронизованы. Точность синхронизации δt должна быть $L \gg \delta t$ ($L = L_l - L_s$ – разность длинного L_l и короткого L_s плеч интерферометра, рис. 2). Точность моментов посылки состояний в канал связи $\approx l \sim 1/\Delta k$.

По существу, плечо интерферометра на передающем конце необходимо для того, чтобы растянуть короткое входное состояние с размером $\sim l$ до более длинного, состоящего из двух "половинок" на расстоянии $L \gg l$. Это технически гораздо проще, чем приготовить исходно протяженное состояние с "длиной" L и, соответственно, с более узким частотным спектром. Канал связи после плеча интерферометра на передающем конце, имеет два оптоволоконных светоделителя, каждый из которых с одним рабочим и "глухим" (вакуумным) входом и выходом, и линии задержки в одном из плеч (рис.2). В канале связи в рабочем выходе состояние имеет вид (с точностью до нормировочного множителя и общей трансляции на длину плеча)

$$|\varphi_{0,1}\rangle + |\varphi_{0,1}(L)\rangle, \qquad (9)$$

где "половинка" состояния задержана на L,

$$|\varphi_{0,1}(L)\rangle = \int d\tau\varphi_{0,1}(\tau - L)|\tau\rangle. \qquad (10)$$

На приемном конце две "половинки" протяженного состояния сводятся вместе обратным унитарным преобразованием, которое реализуется аналогично входному.

Поскольку время начала каждой посылки известно, известна также протяженность состояний L и длина канала связи L_{ch}, то момент достижения детекторов после "собирания" двух половинок на приемном конце также известен. Участник B на приемном конце производит измерения детектором с постоянной времени $\tau_d \ll L$ для того, чтобы фиксировать возможные задержки с точностью лучшей, чем L. То есть не требуется, чтобы детектор различал времена

прилета с точностью l. Иначе говоря, масштабы времен $\approx l$ считаются неразрешимыми (нулевыми).

Призма (или дифракционная решетка) на приемном конце нужна для того, чтобы разделить состояния с разной частотной полосой для 0 и 1. Кроме того, 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 была $\ll L$.

В дальнейшем *в ключе остаются измерения только в тех посылках, которые прошли тест на временную задержку*, то есть такие, которые дали исходы во временном окне $\tau \in (L_s + L_l + L_{ch}) \pm \delta l$ (где δl временное окно в несколько единиц протяженности состояния l). Фактически оставляются только такие *не задержанные* исходы измерений, когда на приемном конце одна "половинка" прошла по длинному плечу, а вторая – по короткому. На приемном конце, наоборот, первая – по короткому, вторая – по длинному. Для таких исходов вероятность того, что подслушиватель знает передаваемый участником A бит и проходит тест на временную задержку, есть

$$\begin{aligned} &\mathrm{Pt}_E(\mathrm{bit}_E = \\ &= \mathrm{bit}_A \wedge \mathrm{test}(\tau \in \tau \in L + L_{ch} + \delta l) = OK) = \\ &\mathrm{Pr}_E(\tau \in \delta l) \cdot 1 \cdot 1 + \mathrm{Pr}_E(\tau \overline{\in} \delta l) \cdot \frac{1}{2} \cdot 1 \leq \\ &\leq \frac{1}{2} \cdot 1 \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} \cdot 1 = \frac{3}{4} < 1. \end{aligned} \tag{11}$$

Первый сомножитель в первом слагаемом есть вероятность регистрации передней половинки одного из состояний. Хотя такая регистрация и приведет к задержке на $\sim l$, однако такие задержки не детектируются. В силу локализованности "половинок" состояний на масштабах l эта вероятность не более $1/2$. Если акт регистрации состоялся, то состояния из-за того, что их частотные полосы не перекрываются, идентифицируются однозначно (второй сомножитель). Третий сомножитель – вероятность пройти временной тест на задержку на приемном конце, равная 1, поскольку постоянная времени детектора $\tau_d \approx> \delta l$. Первый сомножитель во втором слагаемом есть вероятность отсутствия регистрации во временном окне δl. При этом вероятность идентификации состояния равна $1/2$. Третий сомножитель – вероятность пройти тест на временную задержку, вероятность равна 1, поскольку состояние прошло "насквозь" подслушивателя.

Увеличить вероятность идентификации подслушиватель может, лишь дожидаясь второй "половинки" состояния, то есть совершая унитарные преобразования для "собирания" состояния (см. обсуждение выше), что приведет к задержке $\sim L$, которая с вероятностью ~ 1 детектируется. Поскольку участником B будут оставлены только те исходы, которые прошли временной тест на задержку, то исходы с задержкой $\sim L$ выпадут.

Таким образом, для тех измерений, которые прошли временной тест на задержку, вероятность ошибки для подслушивателя составляет

$$\begin{aligned} \delta_E \geq 1 - \mathrm{Pt}_E(\mathrm{bit}_E = \mathrm{bit}_A \wedge \mathrm{test}(\tau \in \tau \in L_s + \\ + L_l + L_{ch} \pm \delta l) = OK) = \frac{1}{4}. \end{aligned} \tag{12}$$

Отметим, что поскольку состояния *ортогональны и все события в протоколе происходят в реальном времени*, то не нужно рассматривать коллективные измерения, поскольку они не увеличивают (12). Невозможность достоверно узнать, что передается, при условии прохождения теста на приемном конце, диктуется квантовостью состояний и ограничениями специальной теории относительности. Кроме того, никакой сторонний шум в канале из-за релятивистских ограничений не может увеличить величину (12) (см. обсуждение выше).

Пусть число посылок, которые прошли тест, есть $2n \gg 1$. Легитимные пользователи выбирают случайно n позиций, раскрывают их, сравнивают значения бит (0 или 1) в каждой позиции и производят оценку вероятности ошибок. Причем данные ошибки могут быть вызваны не подслушивателем, а шумом в канале связи. Важно, что из-за шума величина (12) не может быть превышена. Пусть оценка вероятности ошибки по раскрытой части последовательности есть δ_{AB}. При достаточно длинной последовательности в нераскрытой части вероятность ошибки совпадает с δ_{AB}.

Если же $\delta_{AB} < \delta_E$, то может быть выбран случайный двоичный код $[n, k]$ со скоростью [14,15]

$$k/n \leq R < C(\delta_{AB}) - \varepsilon, \quad \forall \varepsilon > 0, \tag{13}$$

вероятность ошибки которого сколь угодно близка к нулю. Но данный код еще не исправляет ошибки, вероятность которой $\delta_E > \delta_{AB}$. При достаточно длинной последовательности, $n \gg 1$, число одинаковых битов у A и B в результате коррекции есть $\approx nC(\delta_{AB})$, где

$$\begin{aligned} C(\delta_{AB}) &= 1 - H(\delta_{AB}), \\ H(x) &= -x\log x - (1-x)\log(1-x), \end{aligned} \tag{14}$$

$C(x)$ – пропускная способность классического симметричного бинарного канала связи [14, 15].

По сути, при условии $\delta_E > \delta_{AB}$ подслушиватель находится в ситуации, когда скорость передачи превышает пропускную способность канала между A и подслушивателем, которая равна $C(\delta_E)$. Коррекция ошибок при помощи кодов, которые плохи для подслушивателя (то есть при условии $\delta_{AB} < \delta_E$), выглядит для него как передача сообщений со скоростью, превышающей пропускную способность канала связи между A и ним.

В этом случае, при скоростях передачи выше пропускной способности, можно воспользоваться оценкой [16] для вероятности ошибки на символ, которая у подслушивателя не меньше, чем

$$p_E > 1 - 4\frac{\text{const}}{n(C(\delta_{AB}) - C(\delta_E))^2} - \\ - \exp\left\{-\frac{n(C(\delta_{AB}) - C(\delta_E))}{2}\right\}. \qquad (15)$$

Последнее означает, что предельная допустимая вероятность ошибок в канале связи $\delta_{AB} < 1/4 = 25\%$.

После коррекции ошибок, оставшаяся последовательность битов длины $\approx n \cdot C(\delta_{AB})$ у легитимных пользователей одинакова. Подслушиватель со сколь угодно малой вероятностью ошибки может быть знает не более $\approx n \cdot C(\delta_E)$ бит. Число секретных бит, которое могут извлечь легитимные пользователи из своей последовательности длины $\approx n \cdot C(\delta_{AB})$, не более чем, $\approx n \cdot (C(\delta_{AB}) - C(\delta_E))$. Далее сжатием (хэшированием) через открытый канал участники A и B могут усилить секретность ключа, уменьшая длину последовательности. При сжатии ключа можно пользоваться оценкой вероятности ошибки у подслушивателя (15) в исходной последовательности. В итоге возникает ключ с вероятностью единица, одинаковый у легитимных пользователей, и со сколь угодно малой (после сжатия) вероятностью того, что ключ известен подслушивателю.

Характерная собственная постоянная времени τ_d детектора должна быть $l < c \cdot \tau_d \ll L$. Фактически, это требование возникает из-за того, что во временном интервале L необходимо набирать статистику отсчетов для теста на задержку. Детекторы с постоянной времени $\tau_d \approx 10^{-8} \div 10^{-9}$ с являются достаточно стандартными устройствами. При этом длительность (протяженность) входного состояния достаточно иметь $l/c \approx 10 \div 100$ пс ($l = 0.3 \div 3$ см), что с запасом на два порядка $l/c < \tau_d$. Для раздвижки "половинок" состояния достаточно, с запасом на порядок, величины $L \approx 10c \cdot \tau_d \approx 3 \div 30$ м. При этом достаточно точности балансировки плеч на приемном и передающем концах 3 см. В реальных ситуациях оптоволоконная линия связи не является прямой линией, соединяющей участников A и B. Это обстоятельство накладывает некоторое дополнительное ограничение на раздвижку "половинок" состояния. Последняя не может быть меньше, чем $L_{\text{curve}} - L_{\text{ch}}$, где L_{curv} – истинная длина оптоволокна, L_{ch} – длина прямой, соединяющей A и B. Кроме того, поскольку скорость света в оптоволокне c' несколько меньше предельной скорости света в вакууме ($c' < c$), то это приводит к тому, что эффективная длина состояния не может быть меньше, чем $c(L_{\text{curve}} - L_{\text{ch}})/c'$. Также отметим, что криптосистема на частотных состояниях должна быть более устойчивой, чем системы на поляризационных состояниях.

Выражаю благодарность С. С. Назину за полезные обсуждения и критические замечания. Работа поддержана Российским фондом фундаментальных исследований (проект # 02-02-16289), проектами # 40.020.1.1.1170, # 37.029.1.1.0031.

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098; Rev. Mod. Phys., **74**, 145 (2002).
2. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
4. D. Mayers and A. Yao, quant-ph/9802025.
5. E. Biham, M. Boyer, P. O. Boykin et al., quant-ph/9912053.
6. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
7. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
8. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ, **73**, 767 (2001); С. Н. Молотков, Письма в ЖЭТФ **76**, 79 (2002).
9. С. Н. Молотков, ЖЭТФ (в печати).
10. Н. Н. Боголюбов, Д. В. Ширков, *Введение в теорию квантованных полей*, М.: Наука, 1973.
11. Л. Д. Ландау, Р. Пайерлс, Zeits. für Phys. **69**, 56 (1931), *Собрание трудов*, т.1, 1969, М.: Наука, стр. 56.
12. Н. Бор, Л. Розенфельд, Math.-Fys. Medd. **12**, 3 (1933), *Собрание научных трудов*, т.1, 1969, М.: Наука, стр. 39.
13. M. Fleischauer and M. D. Lukin, Phys. Rev. Lett. **84**, 5094 (2000).
14. C. E. Shannon, Bell Syst. Tech. Jour. **28**, 658 (1949).
15. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Company, Amsterdam, New York, Oxord, 1977.
16. J. Wolfowitz, *The Coding Messages Subjected to Chance Errors*, Illinois J. of Math., **1**, 1957, p. 591.