ЖЭТФ, 2011, том 139, вып. 3, стр. 429–439

РЕЛЯТИВИСТСКАЯ КВАНТОВАЯ КРИПТОГРАФИЯ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации
121552, Москва, Россия

Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 28 июня 2010 г.

Предложен новый протокол квантового распределения ключей для передачи ключей через свободное пространство. Протокол, кроме ограничений квантовой механики на различимость неортогональных квантовых состояний, использует дополнительные ограничения, диктуемые специальной теорией относительности. В отличие от всех существующих протоколов квантового распределения ключей, данный протокол обеспечивает секретность ключей при не строго однофотонном источнике квантовых состояний и произвольной длине квантового канала связи.

1. ВВЕДЕНИЕ

Квантовая криптография, точнее, квантовое распределение ключей, позволяет передавать ключи по открытым и доступным для любой модификации квантовым каналам связи. Вспомогательный классический канал связи также доступен для прослушивания, но должен быть аутентичным. Безусловная секретность ключей в квантовой криптографии основана на двух, тесно связанных между собой фундаментальных запретах квантовой механики: запрете копирования неизвестного квантового состояния [1] и невозможности достоверной различимости неортогональных квантовых состояний [2].

В реальной ситуации неоднофотонность источника вместе с потерями в квантовом канале связи приводит к тому, что все базовые протоколы квантового распределения ключей B92 [2], BB84 [3], SARG04 [4], decoy state (с имитирующими состояниями) [5], phase-time coding (фазово-временного кодирования) [6] оказываются неустойчивыми относительно PNS-атаки (photon number splitting) [4] и не гарантируют секретность ключей, если длина квантового канала связи превышает некоторую критическую величину. Отметим, что протокол [6] для оптоволоконных систем квантовой криптографии по сравнению с другими протоколами обеспечивает самую большую длину линии связи.

Протоколы [2–6] используются как в оптоволоконных системах квантовой криптографии, так и в системах, работающих через открытое пространство. Конечной целью работ по квантовой криптографии в открытом пространстве является передача ключей через низкоорбитальные спутники. Важно отметить, что для обеспечения секретности в протоколах [2–6] при длинах, меньших критической, необходимо заранее знать среднее число посылок, достигающих приемной стороны. Если в оптоволоконных системах при заданной длине квантового канала связи можно заранее вычислить потери, то для открытого пространства это уже невозможно.

Возникает принципиальный и практически важный вопрос о том, существуют ли протоколы квантового распределения ключей, которые обеспечивают безусловную секретность ключей при не строго однофотонном источнике и произвольных потерях в квантовом канале связи. Ниже будет предъявлен такой протокол. Данный протокол, кроме ограничений квантовой механики на различимость квантовых состояний, использует дополнительные ограничения, диктуемые специальной теорией относительности.

Ранее в работах [7, 8] были построены протоколы квантовой криптографии, использующие строго од-

*E-mail: molotkov@issp.ac.ru

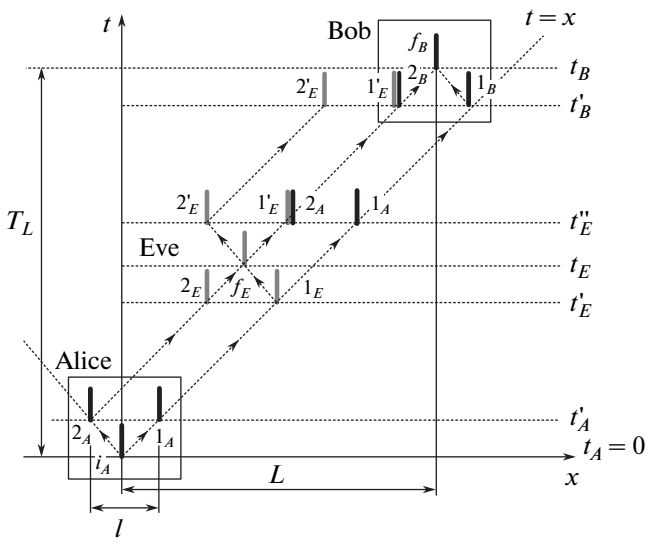

Рис. 1. Пространственно-временная диаграмма, поясняющая работу протокола

нофотонные ортогональные состояния протяженностью, превышающей длину квантового канала связи[1)].

2. ПРОТОКОЛ РЕЛЯТИВИСТСКОГО КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Приведем сначала протокол для однофотонного источника и квантового канала с произвольными потерями, а затем обобщим его на многофотонный случай.

1) Алиса и Боб контролируют области пространства, необходимые для приготовления и детектирования квантовых состояний (рис. 1). Расстояние между точками i_A и f_B известно заранее и равно L (рис. 1). Часы синхронизированы[2)].

2) Алиса готовит в известный момент времени $t_A = 0$ в точке i_A локализованное однофотонное квантовое состояние $|i_A\rangle$. Момент времени $t_A = 0$ считается началом протокола (или отдельной посылки) и всем публично известен.

3) Алиса равновероятно выбирает одно из преобразований, U_A^0, либо U_A^1, переводящее локализованное состояние в момент $t_A = 0$ в одно из протяженных квантовых состояний в момент t'_A. Новое состояние есть суперпозиция пары локализованных состояний с различной относительной фазой φ:

$$|\overline{0}\rangle = U_A^0|i_A\rangle = \frac{1}{\sqrt{2}}(|1_A\rangle + e^{i\varphi}|2_A\rangle),$$
$$|\overline{1}\rangle = U_A^1|i_A\rangle = \frac{1}{\sqrt{2}}(|1_A\rangle - e^{-i\varphi}|2_A\rangle), \quad (1)$$

данные состояния отвечают логическим 0 и 1. Относительная фаза φ всем известна и является параметром протокола. Состояния $|1_A\rangle$ и $|2_A\rangle$ по форме совпадают с $|i_A\rangle$ и отличаются от него только сдвигом в пространстве-времени по двум ветвям светового конуса, выходящим из точки (i_A, t_A) в точки $(1_A, t'_A)$ и $(2_A, t'_A)$ (см. рис. 1):

$$|\overline{0}_A\rangle = \begin{pmatrix} |1_A\rangle\langle i_A| & 0 \\ 0 & e^{i\varphi}|2_A\rangle\langle i_A| \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} |i_A\rangle \\ |i_A\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |1_A\rangle \\ e^{i\varphi}|2_A\rangle \end{pmatrix}, \quad (2)$$

$$|\overline{1}_A\rangle = \begin{pmatrix} |1_A\rangle\langle i_A| & 0 \\ 0 & -e^{-i\varphi}|2_A\rangle\langle i_A| \end{pmatrix} \times \frac{1}{\sqrt{2}} \begin{pmatrix} |i_A\rangle \\ |i_A\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |1_A\rangle \\ -e^{-i\varphi}|2_A\rangle \end{pmatrix}. \quad (3)$$

Верхняя и нижняя строки вектор-столбцов в формулах (2) и (3) отвечают локализованным состояниям в один и тот же момент времени, суперпозиция которых дает единое квантовое состояние. Матрицы (2) и (3) описывают унитарное преобразование в пространстве-времени, подчиняющееся принципу релятивистской причинности. Физически реализуемый унитарный оператор не может содержать матричных элементов между точками, разделенными пространственно-подобным интервалом.

4) С момента t'_A протяженные состояния $|\overline{0}\rangle$ либо $|\overline{1}\rangle$ распространяются со скоростью света на приемную сторону Боба. К моменту времени t'_B они оказываются целиком в области пространства, контролируемой Бобом:

$$|\overline{0}_{t'_B}\rangle = \frac{1}{\sqrt{2}}(|1_{t'B}\rangle + e^{i\varphi}|2_{t'_B}\rangle),$$
$$|\overline{1}_{t'B}\rangle = \frac{1}{\sqrt{2}}(|1_{t'B}\rangle - e^{-i\varphi}|2_{t'_B}\rangle). \quad (4)$$

Боб перед измерением осуществляет унитарное преобразование, преобразующее протяженные квантовые состояния в пространстве-времени в локализованные состояния в точке (f_B, t_B):

[1)] С практической точки зрения протоколы распределения ключей в случаях, когда приходится использовать состояния протяженностью больше длины канала связи, мало интересны.

[2)] Требование синхронизации часов у Алисы и Боба можно снять благодаря двупроходности схемы.

$$|\overline{0}_{t'_B}\rangle = \begin{pmatrix} |f_B\rangle\langle 1_{t'_B}| & 0 \\ 0 & |f_B\rangle\langle 2_{t'_B}| \end{pmatrix} \times \times \frac{1}{\sqrt{2}} \begin{pmatrix} |1_{t'_B}\rangle \\ e^{i\varphi}|2_{t'_B}\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |f_B\rangle \\ e^{i\varphi}|f_B\rangle \end{pmatrix}, \quad (5)$$

$$|\overline{1}_{t'_B}\rangle = \begin{pmatrix} |f_B\rangle\langle 1_{t'_B}| & 0 \\ 0 & |f_B\rangle\langle 2_{t'_B}| \end{pmatrix} \times \times \frac{1}{\sqrt{2}} \begin{pmatrix} |1_{t'_B}\rangle \\ -e^{-i\varphi}|2_{t'_B}\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} |f_B\rangle \\ -e^{-i\varphi}|f_B\rangle \end{pmatrix}. \quad (6)$$

Верхние и нижние строки вектор-столбцов в (5) и (6) отвечают «частям» общего квантового состояния, пришедших в одну пространственно-временную точку (f_B, t_B) по двум ветвям светового конуса (рис. 1). Данное преобразование не зависит от входного состояния Боба. Теперь квантовые состояния (5) и (6) доступны как целое в точке (f_B, t_B). Далее Боб случайно, равновероятно и независимо от Алисы проводит одно из двух локальных измерений. Измерения аналогичны измерениям в стандартном протоколе B92 [2], имеем

$$\begin{aligned} I &= \mathcal{P}_0 + \mathcal{P}_0^{\perp}, \quad \mathcal{P}_{\perp 0} = I - \mathcal{P}_0; \\ I &= \mathcal{P}_1 + \mathcal{P}_1^{\perp}, \quad \mathcal{P}_1^{\perp} = I - \mathcal{P}_1, \end{aligned} \quad (7)$$

$$\begin{aligned} \mathcal{P}_0 &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi} \\ e^{i\varphi} & 1 \end{pmatrix} |f_B\rangle\langle f_B|, \\ \mathcal{P}_1 &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -e^{i\varphi} \\ -e^{-i\varphi} & 1 \end{pmatrix} |f_B\rangle\langle f_B|. \end{aligned} \quad (8)$$

Условная вероятность того, что Алиса посылала 0 (или 1) и Боб получил определенный (conclusive) исход 0 (или 1) есть

$$P\{0_B|0_A\} = \mathrm{Tr}\{|\overline{0}_{t'_B}\rangle\langle\overline{0}_{t'_B}|\mathcal{P}_1^{\perp}\} = = P\{1_B|1_A\} = \mathrm{Tr}\{|\overline{1}_{t'_B}\rangle\langle\overline{1}_{t'_B}|\mathcal{P}_0^{\perp}\} = \cos^2\varphi. \quad (9)$$

Соответственно вероятность исхода с неопределенным результатом есть

$$P\{?_B|0_A\} = \mathrm{Tr}\{|\overline{0}_{t'_B}\rangle\langle\overline{0}_{t'_B}|\mathcal{P}_0\} = = P\{?_B|1_A\} = \mathrm{Tr}\{|\overline{1}_{t'_B}\rangle\langle\overline{1}_{t'_B}|\mathcal{P}_1\} = \sin^2\varphi. \quad (10)$$

Исходы с неопределенным результатом отбрасываются. Боб также отбрасывает все отсчеты, которые задержаны в точке (f_B, t_B) на время, большее $t_B - l/c$ (l — протяженность состояния).

5) Далее часть последовательности раскрывается, оценивается наблюдаемая вероятность ошибки Q_B. Раскрытая часть отбрасывается. Если величина $Q_B < Q_c$ (см. ниже), то ошибки исправляются через открытый канал. Затем для получения финального секретного ключа происходит усиление секретности (сжатие) очищенного ключа универсальными хэш-функциями второго порядка [9].

Скорость света в атмосфере c' слегка отличается от скорости света в вакууме c, что накладывает ограничение на минимальную протяженность состояния l. Для того чтобы Ева не могла скомпенсировать нехватку времени для преобразования состояния, длина состояния должна быть не меньше, чем $l > c(T'_L - T_L)$, где $T_L = (L + l)/c$, $T'_L = (L + l)/c'$, $c' = c/n$, n — показатель преломления. Введя обозначение $\xi = n - 1$, находим $l > \xi L$. Типичная величина ξ в атмосфере на расстоянии приблизительно до 10 км от поверхности Земли для длин волн $\lambda \approx 0.8$ мкм составляет $\xi \approx 10^{-4}$, выше уже практически $c' = c$. Поэтому Ева может скомпенсировать нехватку времени только на данной высоте, заменяя квантовый канал на идеальный (вакуум). Минимальная протяженность состояния l лимитируется этим условием и равна $l \geq \xi \cdot 10[\text{км}] = 1$ м. При такой протяженности состояния передача ключей возможна на любые расстояния.

3. АНАЛИЗ АТАК НА ПЕРЕДАВАЕМЫЙ КЛЮЧ

3.1. Атака прием–перепосыл

Поскольку состояния являются протяженными в пространстве-времени, для их различения Ева должна иметь доступ к состояниям $\frac{1}{\sqrt{2}}(|1_E\rangle \pm e^{\pm i\varphi}|2_E\rangle)$ как целым. Если Ева имеет доступ только к передней «части» состояния $\frac{1}{\sqrt{2}}|1_E\rangle$, то ошибка различения 0 и 1 в точности равна 1/2. Передняя часть состояния является одинаковой для 0 и 1, поэтому вероятность любого измерения не зависит от состояния. Информация заключена в относительной фазе между передней и задней «половинками». Для того чтобы получить доступ ко второй «половинке» состояния $\pm\frac{1}{\sqrt{2}}e^{\pm i\varphi}|2_E\rangle$, Ева должна превратить протяженное в пространстве-времени состояние в состояние, локализованное в точке (f_E, t_E) (рис. 1). Локализованные состояния аналогичны состояниям (5) и (6). Из-за ограничений специальной теорией относительности принципиально невозможно превратить состояние из двух "половинок" в локализованное в точке (f_E, t_E) состояние за время меньшее, чем

высота по времени прошлой части светового конуса, накрывающего данное состояние (рис. 1). Данное ограничение диктуется специальной теорией относительности. Если бы существовал физически реализуемый оператор, преобразующий протяженные состояния в локализованные за меньшее время, то это бы означало, что такой оператор имеет ненулевые матричные элементы, соединяющие точки, разделенные пространственно-подобным интервалом. Последнее означало бы возможность передачи информации быстрее скорости света в вакууме (возможность выхода за световой конус).

После сведения двух «половинок» состояния в точку (f_E, t_E) Ева имеет доступ к состоянию как целому и делает измерения. Из-за неортогональности состояний измерения дают результат с некоторой ошибкой Q_φ. Минимальная ошибка при различении пары неортогональных состояний [10] равна

$$Q_\varphi = \frac{1}{2}(1 - \sqrt{1 - |\langle \overline{0}_A | \overline{1}_A \rangle|^2}) = \frac{1}{2}(1 - \cos\varphi). \quad (11)$$

В зависимости от исхода измерения Ева может приготовить состояние из двух «половинок», аналогичное исходному состоянию Алисы $\frac{1}{\sqrt{2}}(|1'_E\rangle \pm e^{\pm i\varphi}|2'_E\rangle)$. Но из-за ограничений специальной теорией относительности Ева может приготовить протяженное состояние не раньше, чем к моменту t''_E (рис. 1). Однако в момент времени t''_E приготовленное состояние Евы будет отличаться от оригинального состояния Алисы $\frac{1}{\sqrt{2}}(|1_A\rangle \pm e^{\pm\varphi}|2_A\rangle)$ трансляцией в пространстве-времени на величину, равную протяженности состояния, так как исходное состояние Алисы при свободном распространении заняло бы позицию, сдвинутую по времени относительно состояния Евы (см. рис. 1).

Поскольку Боб делает измерения только в определенном временном окне (см. проекторы (7), (8)), сдвинутые по времени состояния Евы дадут одинаковый исход независимо от состояния, из-за того что вторая «половинка» состояния Евы $\pm e^{\pm i\varphi}|2'_E\rangle)$ не успевает к моменту измерений Боба. В результате вероятность ошибки на стороне Боба окажется равной $Q_B = 1/2$.

3.2. Неэффективность «прозрачной» атаки

В нерелятивистской квантовой криптографии наиболее общей и мощной атакой является коллективная атака Евы [11], которая сводится к следующему. Ева в каждой посылке готовит вспомогательное состояние (анциллу), которое приводится во взаимодействие с передаваемым состоянием. После унитарной эволюции анцилла и состояние Алисы оказываются в запутанном состоянии. Возмущенное состояние Алисы направляется к Бобу, а модифицированную анциллу Ева оставляет у себя в квантовой памяти. После передачи всех состояний и измерений на приемной стороне Боба Ева делает коллективные измерения сразу над всеми анциллами в квантовой памяти.

В релятивистском случае такая атака неэффективна и фактически сводится к предыдущей атаке прием–перепосыл. Действительно, пусть совместная эволюция описывается унитарным оператором и, без ограничения общности, может быть представлена в виде

$$\begin{aligned} U_{BE}(|\overline{0}_{t'_E}\rangle \otimes |A\rangle) = \\ = |\overline{0}_{t'_E}\rangle \otimes |\varphi_{00}\rangle + |\overline{1}_{t'_E}\rangle \otimes |\varphi_{01}\rangle, \\ U_{BE}(|\overline{1}_{t'_E}\rangle \otimes |A\rangle) = \\ = |\overline{0}_{t'_E}\rangle \otimes |\varphi_{10}\rangle + |\overline{1}_{t'_E}\rangle \otimes |\varphi_{11}\rangle. \end{aligned} \quad (12)$$

Учитывая, что информационные состояния (1) линейно выражаются через локализованные состояния $|1_{t'_E}\rangle$ и $|2_{t'_E}\rangle$, имеем

$$\begin{aligned} U_{BE}(|1_{t'_E}\rangle \otimes |A\rangle) = \\ = |1_{t'_E}\rangle \otimes |\tilde{\varphi}_{00}\rangle + |2_{t'_E}\rangle \otimes |\tilde{\varphi}_{01}\rangle, \\ U_{BE}(|2_{t'_E}\rangle \otimes |A\rangle) = \\ = |1_{t'_E}\rangle \otimes |\tilde{\varphi}_{10}\rangle + |2_{t'_E}\rangle \otimes |\tilde{\varphi}_{11}\rangle. \end{aligned} \quad (13)$$

Здесь $|\overline{0}_{t'_E}\rangle$, $|\overline{1}_{t'_E}\rangle$ — состояния Алисы в момент t'_E (рис. 1), когда они доступны Еве. Из выражений (12), (13) следует, что унитарный оператор U_{BE} должен иметь следующие ненулевые матричные элементы:

$$\langle 2_{t'_E}|[\langle\tilde{\varphi}_{01}|U_{BE}|A\rangle]|1_{t'_E}\rangle = \langle\tilde{\varphi}_{01}|\tilde{\varphi}_{01}\rangle. \quad (14)$$

Соотношение (14) означает, что если бы преобразование (12), (13) было физически реализуемым, то была возможна мгновенная трансляция в пространстве-времени локализованного состояния $|1_{t'_E}\rangle$ из точки $(1_E, t'_E)$ в состояние $|2_{t'_E}\rangle$ в точке $(2_E, t'_E)$ в тот же самый момент времени t'_E, что противоречит принципу релятивистской причинности. Прозрачная атака возможна, но предварительно Ева должна преобразовать протяженные состояния в одну пространственно-временную точку (f_E, t_E). Затем она должна сделать локальное унитарное преобразование U_{BE} над своей анциллой и преобразованным состоянием Алисы. После можно опять превратить локализованные состояния в протяженные.

Однако это нельзя сделать ранее, чем к моменту времени t''_E. Такие состояния сдвинуты по времени относительно исходных состояний Алисы (рис. 1), что приводит к ошибке на приемной стороне Боба $Q_B = 1/2$ аналогично тому, как это было объяснено в предыдущем разделе.

Ева может сохранить свои анциллы в квантовой памяти и сделать затем коллективные измерения. Это уменьшит ошибку различения последовательности состояний Евы, но модифицированные состояния Боба все равно дадут ошибку $Q_B = 1/2$, так как они сдвинуты по времени относительно исходных состояний Алисы.

3.3. Атака прием–перепосыл с предварительным приготовлением состояния

Существует более эффективная атака, когда Ева предварительно готовит свое состояние $\frac{1}{\sqrt{2}}(|1_A\rangle + |2_A\rangle)$, такое что к моменту времени t_E оно занимает то же положение, что и исходное состояние Алисы. Далее для Евы возможны две стратегии, одна из которых является более эффективной. Тем не менее полезно обсудить обе стратегии.

Эффективность здесь понимается в следующем смысле. Боб всегда исходит из консервативной точки зрения для длины секретного ключа. Для данной наблюдаемой ошибки Q_B на приемной стороне Боб выбирает наименьшую длину секретного ключа при разных стратегиях Евы. Для второй стратегии Евы длина секретного ключа у Боба при данной ошибке Q_B оказывается больше, чем при первой стратегии.

Стратегия 1

Состояние Алисы Ева преобразует в одну точку (f_E, t_E) и делает измерения в этой точке. В зависимости от результата измерений она локально изменяет фазу у второй половинки своего предварительно приготовленного состояния в точке (f_E, t_E). Минимальная ошибка различения неортогональных состояний Алисы есть Q_φ (11), поэтому перепосланное состояние Евы с вероятностью $1 - Q_\varphi$ даст правильный отсчет у Боба в правильный момент времени, а с вероятностью Q_φ отсчет у Боба будет ошибочным, хотя и в правильный момент времени.

Пусть Ева подслушивает долю посылок δ, тогда ошибка на приемной стороне Боба в тех посылках, которые подслушивала Ева, будет равна Q_φ. В остальной доле $1 - \delta$ посылок, которые Ева не подслушивала, ошибка у Боба равна нулю. В тех посылках, которые Ева подслушивала, ошибка равна Q_φ. В доле $1 - \delta$ посылок, которые Ева не подслушивала, ошибка Евы равна $1/2$ — вероятности простого угадывания.

Стратегия 2

Вторая стратегия Евы отличается от первой только на стадии измерений. Состояние Алисы Ева преобразует в одну точку (f_E, t_E) и делает измерения (2) и (3) в этой точке. При этом с вероятностью (9), равной $\cos^2\varphi$, Ева получает результат с определенным исходом (знает передаваемый бит ключа), а с вероятностью (10), равной $\sin^2\varphi$, Ева получает результат с неопределенным исходом. Если Ева получила результат с определенным исходом, то она меняет относительную фазу второй половины состояния по отношению к первой. Для таких посылок на стороне Боба не будет ошибок. Если же Ева получила неопределенный исход, то она может только наугад изменить относительную фазу второй половины состояния по отношению к первой либо попытаться «остановить» (блокировать) состояние, приготовленное заранее. Однако это можно сделать только с вероятностью $1/2$, поскольку Ева уже не имеет доступа к передней половинке состояния. Таким образом, Ева может блокировать только долю $(\delta/2)\sin^2\varphi$ посылок, где был получен исход с неопределенным результатом. Фактически это является следствием нормировки квантового состояния на единицу, т. е. вероятность любого результата измерения в некоторой доступной для измерения пространственно-временно́й области не может быть больше, чем нормировка квантового состояния, которая набирается в этой области. Для доли посылок $(\delta/2)\sin^2\varphi$, которые Ева принципиально не может блокировать, ошибка на приемной стороне Боба будет равна $1/2$. Долю посылок $(\delta/2)\sin^2\varphi$ Ева сумеет блокировать.

3.4. Различие протокола B92 [2] и релятивистского протокола

Отметим еще раз разницу между нерелятивистским протоколом распределения ключей B92 [2] и нашим релятивистским протоколом. В нерелятивистском случае при наличии затухания в канале связи Ева также делает измерения (7), (8). При этом она не должна заранее приготавливать свое состояние, так как момент времени приготовления состояния Алисой и момент времени измерения состояния Бобом не фиксируются. Если Евой получен исход с неопределенным результатом, то она всегда может блокировать посылку, списывая отсутствие состояния на стороне Боба на затухание. Если же получен исход с определенным результатом, то Ева знает со-

стояние Алисы, далее готовит свое состояние и посылает Бобу. При этом ошибок на стороне Боба не возникает. Начиная с некоторой величины затухания в канале связи Ева знает весь передаваемый ключ, не производя ошибок на стороне Боба, т. е. остается не детектируемой. В релятивистской версии протокола такая атака оказывается принципиально невозможной. В оптоволоконных системах квантовой криптографии критическая длина для протокола B92 [2] составляет примерно полтора десятка километров. Причем в канале с затуханием протокол B92 [2] становится несекретным даже при строго однофотонном источнике.

3.5. Длина секретного ключа

Стратегия 1

Пусть переданная последовательность Алисы после отбрасывания исходов с неопределенным (inconclusive) результатом равна $X^N = \{0,1\}^N$. Последовательности Боба и Евы есть $Y^N = \{0,1\}^N$, $E^N = \{0,1\}^N$. Условные вероятности Алиса–Боб, Алиса–Ева для посылок, которые подслушивает Ева, имеют вид

$$\begin{gathered} P(e|x) = P(y|x) = 1 - Q_\varphi, \quad e = y = x; \\ P(e|x) = P(y|x) = Q_\varphi, \quad e, y \neq x. \end{gathered} \tag{15}$$

Соответственно переходные вероятности для посылок, которые Ева не подслушивает, равны

$$\begin{gathered} P(e|x) = \frac{1}{2} \quad \forall e, x; \quad P(y|x) = 1, \quad y = x; \\ P(y|x) = 0, \quad y \neq x. \end{gathered} \tag{16}$$

Согласно работе [11] длина секретного ключа в пределе длинных последовательностей не превосходит

$$\begin{aligned} r &= \min_{all\ attack} \lim_{N\to\infty} \frac{H(E^N|X^N) - H(Y^N|X^N)}{N} = \\ &= \min_{all\ attack} \lim_{N\to\infty} \frac{I(X^N;Y^N) - I(X^N;E^N)}{N}, \end{aligned} \tag{17}$$

где $H(Y^N|X^N)$, $H(E^N|X^N)$, $I(X^N;Y^N)$, $I(X^N;E^N)$ — условные и взаимные информации Алиса–Боб и Алиса–Ева. В длине ключа в выражении (17) (см. [11]) учтено исправление ошибок при помощи случайных шенноновских кодов и усиление секретности очищенного ключа. Поскольку Боб на приемной стороне видит лишь свою наблюдаемую ошибку Q_B, удобно исключить параметр δ, выразив его через наблюдаемую ошибку Боба Q_B, $Q_B = Q_\varphi\delta + 0\cdot(1-\delta)$. Длина секретного ключа в асимптотическом пределе есть

$$\begin{aligned} H(Y^N|X^N) &= -Nh(Q_\varphi), \\ H(E^N|X^N) &= (1-\delta)N - \delta N h(Q_\varphi), \\ r_1 &= 1 - h(Q_B) - \frac{Q_B}{Q_\varphi} + \frac{Q_B}{Q_\varphi} h(Q_\varphi), \end{aligned} \tag{18}$$

где

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x).$$

Наблюдаемая критическая ошибка на приемной стороне Боба, до которой гарантируется секретность передаваемых ключей, определяется из условия $r = 0$ и оказывается равной $Q_c = Q_\varphi$. Напомним, что Q_φ является параметром протокола и определяется степенью неортогональности состояний Алисы (1).

Стратегия 2

С учетом сказанного в предыдущем разделе, для наблюдаемой ошибки на приемной стороне Боба имеем

$$Q_B = \frac{\dfrac{\delta}{2}\sin^2\varphi}{1 - \dfrac{\delta}{2}\sin^2\varphi}.$$

Окончательно для длины секретного ключа после несложных вычислений получаем

$$r_2 = 1 - h(Q_B) - \frac{2(1-2Q_\varphi)^2}{1-(1-2Q_\varphi)^2}\,\frac{Q_B}{(1+Q_B)^2}. \tag{19}$$

Удобно представить зависимость длины секретного ключа для двух стратегий как функцию наблюдаемой ошибки у Боба Q_B при разных значениях угла между сигнальными состояниями (1). На рис. 2 приведены данные зависимости. Как следует из рис. 2, стратегия 1 Евы является более выигрышной, поскольку при данной длине секретного ключа дает меньшую наблюдаемую ошибку. Поэтому предельная критическая ошибка Q_B, до которой гарантируется секретное распределение ключей, должна определяться из соотношения (18) (сплошные кривые на рис. 2).

3.6. Учет потерь в квантовом канале

Ева может извлечь информацию из окружающей среды, где происходит поглощение квантового состояния. Однако из-за специфической протяженной структуры квантовых состояний, состоящих из двух локализованных половинок, поглощение состояния как целого локальным поглотителем возможно лишь за конечное время, требуемое для вхождения

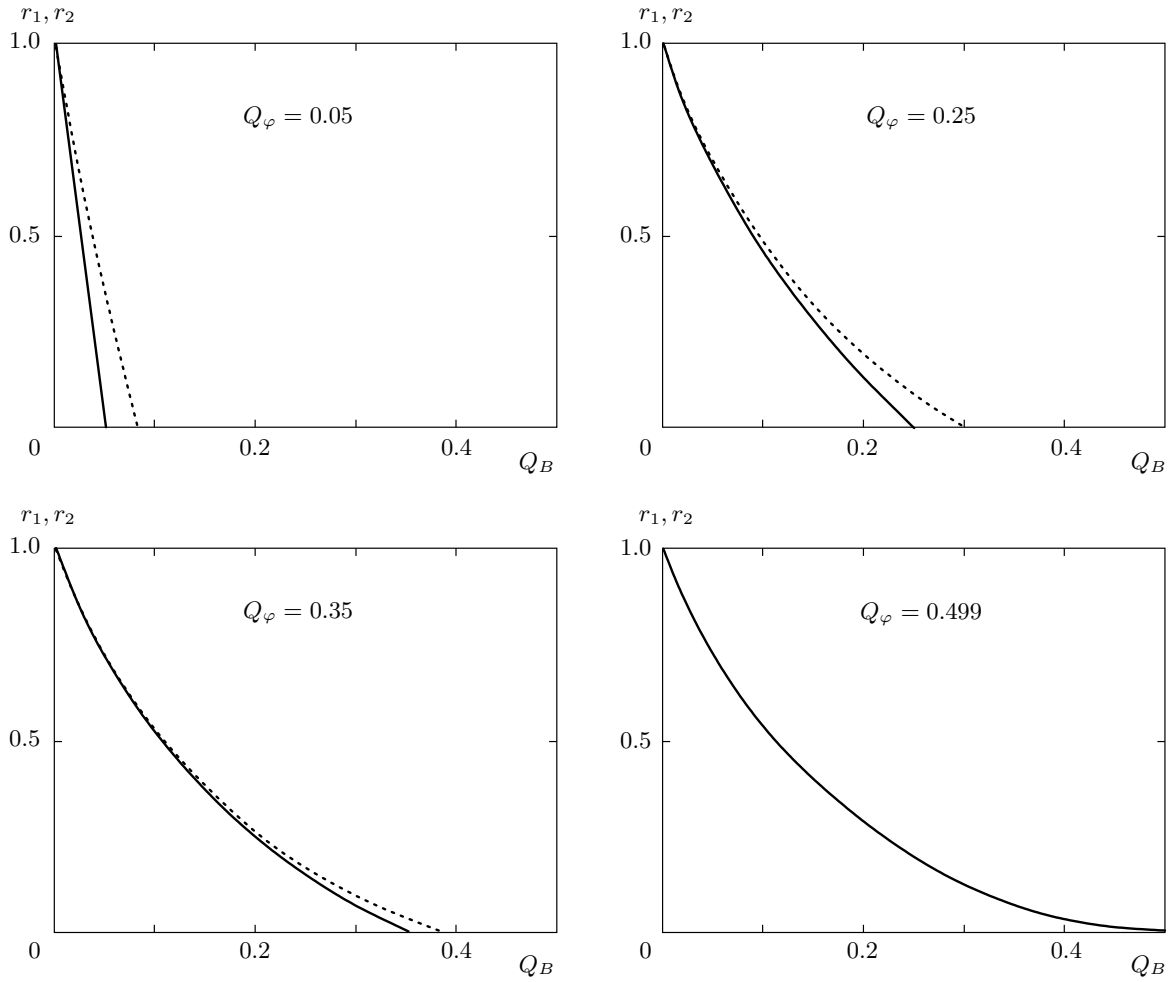

Рис. 2. Зависимости длины секретного ключа в пересчете на одну посылку на приемной стороне как функции наблюдаемой вероятности ошибки Q_B: сплошные линии — r_1, пунктирные — r_2. Величина Q_φ является параметром протокола и связана с углом между информационными квантовыми состояниями формулой (11). Бóльшие значения Q_φ отвечают меньшей различимости информационных квантовых состояний (см. формулу (11))

состояния в поглотитель. После этого Ева может извлечь информацию о поглощенном состоянии из среды, а затем приготовить свое состояние для посылки Бобу. Фактически ситуация аналогична описанной в предыдущих разделах, только теперь преобразование протяженного состояния $\frac{1}{\sqrt{2}}(|1_E\rangle \pm e^{\pm i\varphi}|2_E\rangle)$ в локальное в точке (f_E, t_E) делает сама среда. Из-за неортогональности состояний Ева извлекает информацию из среды с ошибкой не меньше Q_φ, т. е. поглощение в квантовом канале связи аналогично атаке Евы прием–перепосыл. Формально можно представить ситуацию, когда обе — передняя и задняя — «половинки» состояния поглощаются в некоторый момент времени в разных пространственных точках. Однако для того чтобы выяснить, какое состояние поглотилось, необходимо иметь доступ к пространственно-разделенным частям поглотителя, что все равно требует конечного времени l/c.

4. ОПТИЧЕСКАЯ СХЕМА ДЛЯ ПРИГОТОВЛЕНИЯ И ИЗМЕРЕНИЯ СОСТОЯНИЙ

Оптическая схема представлена на рис. 3. Длины всех оптических путей известны и началом каждой посылки является момент приготовления состояния $|1_A\rangle$ Алисой. Данная схема, по сути, реализует преобразование состояний, представленных на диаграмме рис. 1 — растягивание на передающей стороне, а затем сведение в одну точку на приемной стороне.

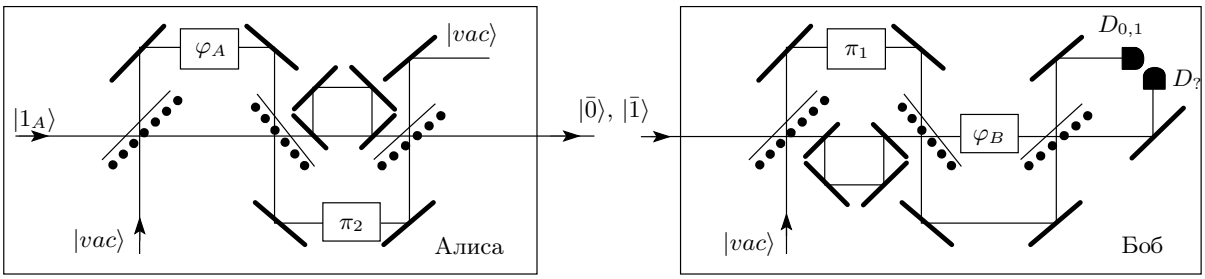

Рис. 3. Оптическая схема для приготовления и регистрации квантовых состояний. Отражающая сторона симметричных светоделителей с изменением знака состояния на π обозначена сплошной линией, без изменения знака — точками

Будем работать в одночастичном подпространстве чисел заполнения. Унитарные операторы, описывающие работу схемы, имеют вид

$$U_s^{\pm} = \frac{1}{\sqrt{2}} \begin{pmatrix} I & \pm I \\ \mp I & I \end{pmatrix},$$
$$U_{\varphi_{A,B}} = \begin{pmatrix} I & 0 \\ 0 & e^{i\varphi_{A,B}} I \end{pmatrix}, \qquad (20)$$
$$U_{j\to j+1} = \begin{pmatrix} \sum\limits_{j=-\infty}^{\infty} |j+1\rangle\langle j| & 0 \\ 0 & I \end{pmatrix},$$

$$U_{\pi_1} = \begin{pmatrix} I & 0 \\ 0 & e^{i\pi}|1\rangle\langle 1| + I(\neq 1) \end{pmatrix},$$
$$U_{\pi_2} = \begin{pmatrix} I & 0 \\ 0 & I(\neq 2) + e^{i\pi}|2\rangle\langle 2| \end{pmatrix}, \qquad (21)$$
$$I(\neq i) = \sum_{j=-\infty, j\neq i}^{\infty} |j\rangle\langle j|.$$

Полный единичный оператор $\overline{I} = |vac\rangle\langle vac| + I$, $I = \sum_{j=-\infty}^{\infty} |j\rangle\langle j|$ — единица в одночастичном подпространстве. Операторы $U_s^{\pm}$ отвечают симметричным светоделителям. Оператор $U_{\varphi_{A,B}}$ отвечает фазовому модулятору, который меняет относительную фазу амплитуды состояний, прошедших по разным путям интерферометра, где $\varphi_{A,B} = \varphi$ для 0 и $\varphi_{A,B} = \pi - \varphi$ для 1. Оператор U_{π_2} описывает фазовый модулятор, который изменяет относительную фазу между состояниями $|1\rangle$ и $|2\rangle$ в суперпозиции только в одном из плеч интерферометра. Физически это реализуется посредством приложения напряжения на фазовый модулятор в момент прохождения второй «половинки» состояния. И наконец, $U_{j\to j+1}$ — оператор сдвига в одном из плеч. Преобразование входного состояния на стороне Алисы имеет вид

$$U_s^+ U_{\pi_2} U_s^- U_{\varphi_A} U_{j\to j+1} U_s^+ \begin{pmatrix} |1_A\rangle \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} (|1_A\rangle + e^{i\varphi_A}|2_A\rangle) \\ 0 \end{pmatrix}. \qquad (22)$$

На приемной стороне преобразования Боба имеют вид

$$U_s^+ U_{\varphi_B} U_{j\to j+1} U_s^- U_{\pi_1} U_s^+ \times \frac{1}{\sqrt{2}} \begin{pmatrix} (|1_A\rangle + e^{i\varphi_A}|2_B\rangle) \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} (e^{i\varphi_A} + e^{i\varphi_B})|2_B\rangle \\ -(e^{i\varphi_A} - e^{i\varphi_B})|2_B\rangle \end{pmatrix}. \qquad (23)$$

Если Алиса посылала 0 — $\varphi_A = \varphi$ и Боб выбрал $\varphi_B = \varphi$, то вероятность отсчета в $D_{0,1}$ тождественно равна нулю, а в $D_?$ — единице. Аналогично, если Алиса посылала 1 — $\varphi_A = \pi - \varphi$ и фаза Боба $\varphi_B = \pi - \varphi$, то имеет место аналогичная ситуация. Если же Алиса посылала 0, а Боб выбрал фазу $\varphi_B = \pi - \varphi$, то вероятность отсчета в $D_{0,1}$ равна $\cos^2\varphi$. Аналогично в случае, когда Алиса посылала 1, а Боб выбрал фазу $\varphi_B = \varphi$. Вероятность определенных (conclusive) отсчетов в детекторе $D_{0,1}$ равна $\cos^2\varphi$, вероятность исходов с неопределенным результатом в $D_?$ — $\sin^2\varphi$.

5. МНОГОФОТОННЫЙ СЛУЧАЙ

Пусть исходные состояния Алисы представляют собой ослабленное лазерное излучение — когерент-

ное состояние со средним числом фотонов $\mu = |\alpha|^2$:

$$|\overline{0}_\alpha\rangle_A = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n_{\overline{0}}\rangle_A,$$
$$|\overline{1}_\alpha\rangle_A = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n_{\overline{1}}\rangle_A, \quad |n_{\overline{0}}\rangle_A = |\overline{0}\rangle_A^{\otimes n}, \quad (24)$$
$$|n_{\overline{1}}\rangle_A = |\overline{1}\rangle_A^{\otimes n}, \quad |n_{\overline{0,1}}\rangle_A = |vac\rangle, \quad n = 0.$$

Ева может использовать все предыдущие атаки, однако есть более эффективная. Ева может расщепить состояние Алисы, используя светоделитель. Пусть коэффициент светоделителя η. Поскольку светоделителем когерентное состояние преобразуется подобным образом, состояния Евы и Боба имеют вид

$$|\overline{0}_{\alpha\sqrt{1-\eta}}\rangle_E \otimes |\overline{0}_{\alpha\sqrt{\eta}}\rangle_B, \quad |\overline{1}_{\alpha\sqrt{1-\eta}}\rangle_E \otimes |\overline{1}_{\alpha\sqrt{\eta}}\rangle_B.$$

В этом случае Ева не производит ни задержки, ни ошибки на стороне Боба. Ева сохраняет свои состояния в квантовой памяти и проводит коллективные измерения в самом конце протокола над целой последовательностью, исключая естественно посылки, в которых Боб получил результаты с неопределенным исходом. Боб подвергает свои состояния преобразованиям, аналогичным в (20)–(23). В результате состояния перед входом в детекторы оказываются равными

$$\begin{pmatrix} |2_{\alpha_+(\varphi_A,\varphi_B)}\rangle_B \\ |2_{\alpha_-(\varphi_A,\varphi_B)}\rangle_B \end{pmatrix}, \quad |2_{\alpha_\pm(\varphi_A,\varphi_B)}\rangle_B =$$
$$= \exp\left\{-\frac{|\alpha_\pm(\varphi_A,\varphi_B)|^2}{2}\right\}\times$$
$$\times\sum_{n=0}^{\infty}\frac{\alpha_\pm(\varphi_A,\varphi_B)^n}{\sqrt{n!}}|2_B\rangle^{\otimes n}, \quad (25)$$

$$\alpha_\pm(\varphi_A,\varphi_B) = \pm\alpha\sqrt{\eta}\frac{e^{i\varphi_A}\pm e^{i\varphi_B}}{2}.$$

Считаем, как обычно, что детекторы Боба не различают число фотонов и не реагируют на вакуумную компоненту состояния. Вероятность определенных (conclusive) исходов в $D_{0,1}$ равна

$$e^{-\mu}(e^{\mu\eta\cos^2\varphi}-1)$$

и вероятность исходов с неопределенным результатом —

$$e^{-\mu}(e^{\mu\eta\sin^2\varphi}-1).$$

Классическая информация Евы ограничена величиной Холево [12] для ансамбля матриц плотности

$$\rho_{0_{\sqrt{1-\eta}\alpha}} = |\overline{0}_{\sqrt{1-\eta}\alpha}\rangle_{EE}\langle\overline{0}_{\sqrt{1-\eta}\alpha}|,$$

$$\rho_{1_{\sqrt{1-\eta}\alpha}} = |\overline{1}_{\sqrt{1-\eta}\alpha}\rangle_{EE}\langle\overline{1}_{\sqrt{1-\eta}\alpha}|,$$

которая равна

$$\chi(\rho_{\sqrt{1-\eta}\alpha}) \le S\left(\frac{1}{2}\left(\rho_{0_{\sqrt{1-\eta}\alpha}}+\rho_{1_{\sqrt{1-\eta}\alpha}}\right)\right) -$$
$$-\frac{1}{2}\left(S(\rho_{0_{\sqrt{1-\eta}\alpha}})+S(\rho_{1_{\sqrt{1-\eta}\alpha}})\right) <$$
$$< \lim_{\eta\to 0}\chi(\rho_{\sqrt{1-\eta}\alpha}) = \chi(\rho_\alpha), \quad (26)$$

где $S(\rho)$ — энтропия фон Неймана. Окончательно имеем

$$\chi(\rho_\alpha) = \overline{C}(\rho_\alpha) = -\frac{1+\varepsilon}{2}\log_2\frac{1+\varepsilon}{2} - \frac{1-\varepsilon}{2}\times$$
$$\times\log_2\frac{1-\varepsilon}{2}, \quad \varepsilon = |_A\langle\overline{0}_\alpha|\overline{1}_\alpha\rangle_A| = e^{-\mu\cos^2\varphi}. \quad (27)$$

Здесь $\overline{C}(\rho_\alpha)$ — классическая пропускная способность квантового канала связи Алиса–Ева. Фактически Ева как бы отводит все фотоны себе, а остальные через свой идеальный канал направляет к Бобу. Отметим, что Боб не должен следить за средним числом долетевших до него посылок. Боб делает измерения, аналогичные однофотонному случаю. Поскольку нет ошибок, после отбрасывания неопределенных исходов, находим $I(Y^N|X^N) = N$ (N — число посылок, давших определенный (conclusive) исход). Длина секретного ключа (точнее, доля секретных битов на каждую не отброшенную посылку) не превышает

$$r = \min_{all\ attack}\lim_{N\to\infty}\left(\frac{I(Y^N|X^N)-N\chi(\rho_\alpha)}{N}\right) =$$
$$= 1-\overline{C}(\rho_\alpha). \quad (28)$$

При больших средних числах фотонов в состоянии длина секретного ключа быстро стремится к нулю $r \propto e^{-\mu\cos^2\varphi}$, однако никогда не обращается в нуль. Формально секретность гарантируется при любых μ, но скорость генерации ключа экспоненциально быстро уменьшается (например, $\mu = 1$, $r \approx 0.37N$; $\mu = 2$, $r \approx 0.14N$). Важно, что в критерий секретности затухание вообще не входит, длина ключа зависит только от исходных квантовых состояний. Анализ потерь в квантовом канале связи сводится к предыдущему случаю. В многофотонном случае Ева сама выполняет роль поглотителя, отводя часть состояния. Однако из-за неортогональности состояний Ева не может получить достоверные исходы в каждой посылке, в отличие от Боба, который отбрасывает исходы с неопределенным результатом. Многофотонность лишь уменьшает ошибку различения у

Таблица

	B92	BB84	SARG04	Decoy state	Phase-time coding	Релятивистская квантовая криптография
Однофотонный источник, канал связи без потерь, идеальные детекторы	+	+	+	+	+	+
Однофотонный источник, канал связи с потерями, идеальные детекторы	$L < L_1$	+	+	+	+	+
Неоднофотонный источник, канал связи с потерями, идеальные детекторы	$L < L_1$	$L < L_2$	$L < L_3$	$L < L_4$	$L < L_5$	+
Неоднофотонный источник, канал связи с потерями, неидеальные детекторы	$L < L_1$	$L < L_2$	$L < L_3$	$L < L_4$	$L < L_5$	$L < L_6$

Евы по сравнению с индивидуальными измерениями (11). Попытка сначала измерять многофотонные состояния, а затем перепосылать Бобу приведет к задержке перепосланных состояний и ошибке у Боба, равной 1/2, аналогично однофотонному случаю.

6. СРАВНЕНИЕ СТОЙКОСТИ РАЗЛИЧНЫХ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Приведем сравнительные данные по стойкости базовых протоколов квантового распределения ключей, секретность которых основана только на запретах квантовой механики, и предложенного релятивистского протокола, секретность которого гарантируется фундаментальными запретами квантовой механики и специальной теорией относительности.

Данные сведены в таблицу. В случае строго однофотонного источника, квантового канала связи без потерь и идеальных фотодетекторов все протоколы обеспечивают секретность ключей при любых длинах линии связи (первая строка таблицы). Под идеальными детекторами здесь понимаются детекторы, не имеющие собственных темновых шумов.

При потерях в квантовом канале связи, но строго однофотонном источнике и идеальных детекторах протокол B92 обеспечивает секретность ключей, лишь если длина квантового канала связи не превышает критическую длину L_1. Оценки длины линии связи для одномодового оптоволокна SMF-28 дают величину критической длины $L_1 < 15$–18 км. Все остальные протоколы обеспечивают секретность при любых длинах квантового канала связи.

В третьей строке приведены данные для неоднофотонного источника, канала связи с потерями и идеальных детекторов. В этом случае все протоколы, кроме релятивистского, теряют секретность при длинах, больших критической, причем $L_1 < L_2 < L_3 < L_4 < L_5$. Потеря секретности протоколов (кроме B92) происходит фактически из-за того, что подслушиватель может неразрушающим способом определять число фотонов в канале связи. В релятивистском случае для измерения числа фотонов с вероятностью единица требуется доступ ко всему состоянию, поскольку квантовое состояние нормировано, что с учетом ограничений специальной теории относительности не может быть сделано мгновенно. Такое измерение приводит к неизбежным задержкам, которые и детектируются.

В последней строке таблицы приведены данные для случая неоднофотонного источника, канала связи с потерями и неидеальных детекторов. В этом случае все протоколы имеют ограничение по длине линии связи. В релятивистском случае ограничение по длине происходит фактически из-за того, что при больших длинах (соответственно, потерях) в канале связи все меньшее число посылок достигает приемной стороны. В пределе, когда ни одна посылка не доходит до приемной стороны, на ней регистрируются только случайные темновые шумы детекто-

ров, которые приводят к ошибке в 50 %. Такая ошибка есть теоретический предел для бинарного канала связи, до которой вообще можно передавать информацию. В квантовой криптографии ошибки требуется исправить через открытый классический канал связи. При вероятности ошибки 50 % вся длина последовательности расходуется на исправление ошибок, поэтому для секретного ключа просто ничего не остается.

7. ЗАКЛЮЧЕНИЕ

Учет фундаментальных ограничений, накладываемых специальной теорией относительности на измеримость неортогональных квантовых состояний, приводит к тому, что возможна передача секретных ключей на любые расстояния через открытое пространство даже при не строго однофотонном источнике и любых потерях в канале связи.

Здесь мы ограничились идеальными детекторами у Боба. Учет темновых шумов может привести к дополнительным ограничениям. Однако напомним, что нерелятивистские протоколы [3–6] при не строго однофотонном источнике и потерях в канале связи, больших критических, становятся несекретными даже при идеальных детекторах. В релятивистском случае данного ограничения нет.

Автор выражает благодарность коллегам по Академии криптографии РФ за постоянную поддержку.

Работа выполнена при частичной финансовой поддержке РФФИ (грант № 08-02-00559).

ЛИТЕРАТУРА

1. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. lett. **68**, 3121 (1992).
3. C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. Comput. Sys. Sign. Proces., Bangalore, India (1984), p. 175.
4. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901-1 (2004).
5. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).
6. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).
7. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
8. M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
9. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
10. C. W. Helstrom, *Quantum Detection and Estimation Theory*, Acad. Press, New York, San Francisco, London (1976).
11. R. Renner, arXiv:quant-ph/0512258.
12. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Совр. матем. физ.*, вып. 5, МЦНМО, Москва (2002); УМН **53**, 193 (1998).