Письма в ЖЭТФ, том 64, вып.9, стр.652 - 657 © 1996г. 10 ноября

# ВЛИЯНИЕ ДИСПЕРСИИ И ЗАТУХАНИЯ В КАНАЛЕ СВЯЗИ НА СЕКРЕТНОСТЬ КВАНТОВОЙ КРИПТОСИСТЕМЫ

*С.Н.Молотков*

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

Поступила в редакцию 8 октября 1996 г.

Исследовано влияние дисперсии канала связи на секретность квантовой криптосистемы, основанной на использовании однофотонных состояний с различными частотами. Найдена критическая длина канала связи, при которой еще может быть обеспечена конфиденциальность распространения ключа.

PACS: 03.65.Bz, 42.50.Wm, 89.70.+c,

Основная задача криптографии состоит в обмене секретной информацией между двумя или несколькими законными пользователями. Главным элементом любой криптосистемы является ключ – случайная последовательность нулей и единиц, которая используется для кодирования сообщений [1]. Если длина ключа равна длине сообщения и ключ известен только законным пользователям A и B, и используется только раз, то сообщения являются полностью конфиденциальными [2]. Поэтому основной проблемой является обеспечение секретности распространения ключа между законными пользователями. В обычной криптографии не существует фундаментального запрета на подсматривание ключа во время его распространения, и секретность криптосистемы базируется на вычислительной сложности кода, а не на фундаментальных законах природы [1].

Квантовая криптография дает регулярный способ распространения ключа, причем секретность распространения основывается на фундаментальных законах природы (квантовой механики).

Как правило, секретность квантовых криптосистем доказывается для идеальных каналов связи. Неидеальность канала связи в принципе должна снижать секретность при распространении ключа, поэтому для любой практической криптосистемы необходим учет неидеальности канала связи.

В последнее время было предложено несколько квантовых криптосистем [3-9]. Одна из систем, использующая фазовое кодирование и оптоволоконную линию связи, была реализована экспериментально на расстоянии 30 км [9]. Схема [9] представляет собой оптоволоконный интерферометр с длиной базы 30 км.

В работе [10] была предложена квантовая криптосистема, основанная на EPR-эффекте (Эйнштейна – Подольского – Розена) для бифотонных состояний. Оказывается, что подобная схема может быть реализована с использованием однофотонных состояний, что гораздо проще реализовать экспериментально, поскольку не требуется генерации бифотонных состояний (например, при помощи параметрических процессов). *Кроме того, данная схема должна быть гораздо более устойчивой, поскольку не использует оптоволоконный интерферометр с длинной базой.*

Секретность криптосистемы (детектирование попыток подслушивания) гарантируется фундаментальным соотношением неопределенностей энергия–время. Предложенная в [10] схема не учитывала дисперсии и затухания

в линии связи, что может оказаться критическим обстоятельством при экспериментальной реализации. Целью данной работы является выяснение условий, при которых при наличии дисперсии и затухания квантовая криптосистема остается секретной.

Опишем сначала протокол генерации ключа без использования бифотонных состояний. Протокол генерации ключа состоит в следующем. Пользователь A случайным образом и в случайные моменты времени посылает в линию связи к пользователю B один из трех сигналов: один из двух однофотонных сигналов с узким частотным спектром (сигналы с хорошо определенными частотами $\omega_1$ или $\omega_2$, ширины спектра которых $\sigma_1$ и $\sigma_2$, соответственно, малы) либо один однофотонный с короткой по времени длительностью сигнал, спектр которого достаточно широк ($\sigma_\infty$). Несущая частота $\omega_0 \approx \omega_{1,2}$. Для реальных параметров окну прозрачности оптоволокна отвечает длина волны $\lambda \approx 1.3$ мкм (соответствующие частоты $\omega_{0,1,2} \approx 10^{15}$ с$^{-1}$).

Посылка сигналов с хорошо определенной частотой $\omega_1$ или $\omega_2$ означает, что разброс времен вылета ($\Delta t$) у A и приема у B известен с плохой точностью, не лучшей, чем $\Delta t \geq 1/\sigma_{1,2}$. Последнее гарантируется фундаментальным соотношением неопределенностей энергия–время.

В случае посылки фотона с широким спектром состояние может быть приготовлено быстро, но при этом неопределенность по частоте $\sigma_\infty$ велика, но зато с хорошей точностью может быть измерено время ($\Delta t$) вылета (приема) фотона ($\Delta t \approx 1/\sigma_\infty \to 0$, при $\sigma_\infty \to \infty$).

Далее регистрирующие приборы будем условно называть фотодетекторами. Пользователь B случайно и независимо от A в каждом измерении выбирает один из двух узкополосных фотодетекторов с центральными частотами $\omega_1$ или $\omega_2$ и шириной $\gamma_{1,2} \approx \sigma_{1,2}$, либо широкополосный с центральной частотой $\omega_0$ и полосой детектирования $\gamma_\infty \approx \sigma_\infty$. Расстояния по частоте $\delta\omega_{12} = |\omega_1 - \omega_2|$ должно быть не меньше суммы дисперсий $\sigma_1$ и $\sigma_2$, иначе сигналы с $\omega_1$ и $\omega_2$ невозможно отличить. При гауссовой форме спектра достаточно, чтобы $\delta\omega_{12}$ составляла не меньше $3(\sigma_1 + \sigma_2)$.

Измерения узкополосным фотодетектором позволяют отличить $\omega_1$ от $\omega_2$, но такие измерения (и, соответственно, *приготовление состояний*) не могут быть сделаны за время меньшее, чем $\Delta t_{1,2} \geq 1/\delta\omega_{12}$ ($\Delta t_{12}$ – разброс времен измерений).

Измерения широкополосным фотодетектором могут быть проведены за время $\Delta t_\infty \approx 1/\sigma_\infty \to 0$, но при этом ничего (с точностью лучшей, чем $\sigma_\infty$) нельзя сказать о частоте фотона. Пользователи A и B выбирают параметры так, чтобы выполнялось соотношение

$$\Delta t_\infty \ll \Delta t_{12}. \tag{1}$$

После проведения серии измерений A и B через открытый канал связи сообщают, какой тип фотодетектора (узкополосный или широкополосный) использовался в каждом измерении, но в случае узкополосных не сообщают, какой именно, с частотой $\omega_1$ или $\omega_2$, использовался. Те измерения, где не было срабатывания фотодетекторов или не было совпадения типа, отбрасываются. Оставшиеся измерения, где использовались узкополосные фотодетекторы, дают случайную и идентичную последовательность, которая может быть использована в качестве ключа ($\omega_1$ соответствует логическому нулю, а $\omega_2$ – единице). Вероятность сбоя (перепутывания нуля и единицы) ничтожно мала при $\delta\omega_{12} > 3(\sigma_1 + \sigma_2)$. Для коррекции ключа может быть в дальнейшем

использован метод privacy amplification scheme, предложенный Беннетом и др. [11].

Измерения, где использовались короткие импульсы (известно с большой точностью время вылета и прилета фотона), служат для обнаружения попыток подслушивания. Для этих измерений сообщаются через открытый канал связи время посылки сигнала пользователем A ($t_A$) и время приема у B ($t_B$). Длина линии считается известной, тогда время задержки $t_A - t_B = \mathrm{const}$ (с точностью $\Delta t_\infty \approx 1/\sigma_\infty \to 0$). Систематическое отклонение $t_A - t_B$ от номинала указывает на присутствие подслушивателя в линии связи. Действительно, чтобы извлечь информацию о ключе, подслушиватель должен отличать $\omega_1$ от $\omega_2$ (0 или 1), для этого он должен проводить измерения узкополосным фотодетектором. Такие измерения (а также *приготовление* узкополосных сигналов с $\omega_1$ и $\omega_2$ для перепосыла их к B) не могут быть проведены за времена, меньшие, чем $\Delta t_{12} \approx 1/\delta\omega_{12} \gg \Delta t_\infty$. Неизбежно подслушиватель попадет на ситуации (из-за случайного выбора типа посылок пользователем A), когда A посылал короткие по времени сигналы, а подслушиватель измерял узкополосным фотодетектором, а затем перепосылал к B сигнал с хорошо определенной частотой. Перепосылка сигнала к B необходима, иначе это измерение будет отброшено из-за несрабатывания фотодетектора у B. Данное обстоятельство приведет к систематическому отклонению $t_A - t_B$ от номинала на величину $\Delta t_{12} \approx 1/\delta\omega_{12}$ гораздо большую, чем точность, с которой известна разность $t_A - t_B$ пользователям A и B.

Пока все рассуждения не учитывали затухания и дисперсии квантового канала связи. Реально в качестве такого канала связи используется оптоволокно, поэтому короткие по времени сигналы, посылаемые пользователем A, будут расплываться (продолжительность сигнала на приемном конце возрастает), что может привести к ухудшению точности фиксации прилета фотона у пользователя B, облегчая тем самым ситуацию для подслушивателя и снижая секретность криптосистемы.

Нашей целью будет выяснение соотношений между параметрами однофотонных состояний $\sigma_{1,2}$, $\delta\omega_{12}$, $\sigma_\infty$, дисперсией и затуханием в канале связи, при которых еще может быть обеспечена конфиденциальность распространения ключа.

Пусть пользователь A готовит однофотонное состояние на входе в канал связи (точка $x = 0$) с шириной спектра по частоте $\sigma$ (где $\sigma$ одна из $\sigma_{1,2,\infty}$) на несущей частоте $\omega_0$ (считаем для определенности $\omega_0 = \omega_{1,2}$, хотя это не существенно):

$$E(0,t) = \frac{1}{(\pi\sigma^2)^{1/4}} \int_0^\infty \exp\left\{-\frac{(\omega-\omega_0)^2}{2\sigma^2}\right\} \exp(-i\omega t)d\omega. \tag{2}$$

Эффективная длительность импульса на входе в линию

$$(\Delta t_A)^2 = \int_0^\infty (t-\bar{t})^2 |E(0,t)|^2 dt = \frac{1}{2\sigma^2}, \tag{3}$$

$$\bar{t} = \int_0^\infty t|E(0,t)|^2 dt,$$

и ширина спектра

$$(\Delta\omega_A)^2 = \int_0^\infty (\omega-\bar{\omega})^2 |E(0,\omega)|^2 d\omega = \sigma^2/2, \tag{4}$$

$$\overline{\omega} = \int_0^\infty \omega |E(0,\omega)|^2 d\omega,$$

$$E(0,\omega) = \int_0^\infty E(0,t) \exp(i\omega t) dt.$$

Реально даже для короткого по времени сигнала $\bar{t} \approx 10^{-12}$ с ширина спектра по частоте (несущая частота $\omega_0$) $\approx 10^{15}$ с$^{-1}$, поэтому при учете дисперсии можно ограничиться квадратичным разложением волнового вектора по частоте [12,13]

$$k(\omega) = k_0 + \alpha(\omega - \omega_0) + \beta(\omega - \omega_0)^2, \tag{5}$$

где $\alpha$ и $\beta$ – в общем случае комплексные константы; мнимая часть описывает затухание, вещественная – дисперсию. Пусть сначала затухание отсутствует (затухание учтем позднее). На приемном конце линии у B (точка $x$) сигнал (2) принимает вид

$$E(x,t) = \frac{1}{2\sqrt{\pi}} \frac{1}{\sqrt{\sigma_0^2 - i\beta x}} \exp\left\{-\frac{(\alpha x - t)^2}{4(\sigma_0^2 - i\beta x)}\right\}, \quad \sigma_0^2 = \frac{1}{2\sigma^2}. \tag{6}$$

Интенсивность поля у пользователя B равна

$$|E(x,t)|^2 = \frac{1}{4\pi(\sigma_0^2 + \beta^2 x^2)} \exp\left\{-\frac{(\alpha x - t)^2}{2\sigma^2(x)}\right\}, \quad \sigma^2(x) = \frac{\sigma_0^4 + \beta^2 x^2}{2\sigma_0^2}. \tag{7}$$

Эффективная ширина спектра по частоте в точке $x$ остается такой же, как и на входе в линию (затухание пока не учитываем):

$$(\Delta\omega_A)^2 = (\Delta\omega_B)^2 = \int_0^\infty (\omega - \overline{\omega})^2 |E(0,\omega)|^2 d\omega = \int_0^\infty (\omega - \overline{\omega})^2 |E(x,\omega)|^2 d\omega. \tag{8}$$

Эффективная длительность по времени на приемном конце увеличивается:

$$(\Delta t_B)^2 = \int_0^\infty (t - \bar{t})^2 |E(x,t)|^2 dt = \frac{1}{2\sigma^2(x)} = \frac{1}{2\sigma^2}(1 + \beta^2 x^2 \sigma^4), \tag{9}$$

увеличение происходит в $(1 + \beta^2 x^2 \sigma^4)$ раз. Данное время $\Delta t_B$ представляет собой среднее время прохождения волнового пакета через точку $x$, а неравенство

$$\Delta\omega_B \Delta t_B \geq \sqrt{1 + \beta^2 x^2 \sigma^4} \tag{10}$$

представляет собой вариант неравенств Мандельштама–Тамма [14]. Соотношение (10) описывает статистику опытов (потенциальных), производимых над частицей. Данное соотношение еще не описывает реального процесса измерения над фотоном, поэтому оно не представляет собой соотношения неопределенностей энергия–время, имеющего место в реальном измерении (такие реальные измерения описываются соотношением Бора [15], см. подробные обсуждения в работе Крылова и Фока [16]). Здесь мы будем придерживаться ортодоксальной точки зрения, считая, что соотношение неопределенностей энергия–время представляет собой фундаментальный закон природы (обсуждение различных точек зрения см. в обзоре Додонова и Манько [17]). Среднее время $\Delta t_B$ прохождения волнового пакета через точку $x$ никак не связано с временем измерения $\delta t$, которое устанавливается экспериментатором. Соотношение Бора относится к реальному процессу измерения (например, прохождению частицы

через затвор прибора), действие которого неизбежно связано с неконтролируемым изменением состояния энергии частицы

$$\Delta E \Delta t \geq 1, \tag{11}$$

где $\Delta E$ – разброс энергий, получаемый при измерении [17]. Соотношение Бора является, по-существу, постулатом, поскольку процесс измерения не описывается уравнением Шредингера в отличие от соотношения Мандельштама–Тамма, которое выводится из свободной эволюции пакета, подчиняющейся уравнению Шредингера [14].

Таким образом, для регистрации фотона с шириной спектра $\sigma_\infty$ пользователь B должен открывать диафрагму на время, не меньшее $(1+\beta^2 x^2 \sigma_\infty^4)^{1/2}/\sigma_\infty$. Пользователь B может регистрировать время прилета фотона с той же точностью, что и в линии без дисперсии, открывая диафрагму на время порядка $(1+\beta^2 x^2 \sigma_\infty^4)^{1/2}/\sigma_\infty$. Грубо говоря, из-за расплывания пакета на приемном конце фотон за то же время (как это было в линии без дисперсии) не успевает пройти через диафрагму. Конечно пользователь B мог бы открывать диафрагму на сколь угодно малое время, однако при этом систематически невозможно регистрировать фотон. Именно систематически, в отдельном измерении может иметь место регистрация даже при времени открытия $\delta t \to 0$, но на большом числе измерений такая доля стремится к нулю, противное противоречило бы соотношению неопределенностей Бора энергия–время [15].

Выясним теперь условия, при которых квантовая криптосистема остается секретной. Для этого разброс времен регистрации у пользователя B для коротких импульсов $\Delta t_B$ должен быть заметно меньше, чем время, требуемое подслушивателю (находящемуся в точке $x_E$ между A и B) для регистрации фотонов узкополосным фотодетектором, которое, по обсуждавшимся выше причинам, не может быть сделано короче, чем

$$\Delta t_E \geq \frac{(1+\beta^2 x_E^2 \sigma_{1,2}^4)^{1/2}}{\delta\omega_{12}}. \tag{12}$$

Из неравенства

$$\Delta t_B \ll \Delta t_E \tag{13}$$

следует ограничение на длину линии

$$\frac{(1+\beta^2 x^2 \sigma_\infty^4)^{1/2}}{\sigma_\infty} \ll \frac{(1+\beta^2 x_E^2 \sigma_{1,2}^4)^{1/2}}{\delta\omega_{12}}. \tag{14}$$

Наиболее невыгодная ситуация для секретности возникает, когда подслушиватель находится вблизи пользователя A ($x_E \approx 0$), в этом случае расплывание пакета у подслушивателя не происходит. В итоге имеем ограничение на длину канала связи

$$x_B \leq \frac{1}{\delta\omega_{12}\sigma_\infty\beta}. \tag{15}$$

Таким образом, чем меньше расстояние по частоте между импульсами $\omega_1$ и $\omega_2$, несущими информацию, и чем короче по времени контрольный импульс (чем шире его спектр по частоте), и чем меньше квадратичный коэффициент дисперсии, тем при большей длине квантового канала связи система остается секретной. Данное неравенство не является лимитирующим для длины линии. Длина линии формально может быть сделана сколь угодно большой, однако

при этом платой за увеличение длины линии будет уменьшение расстояния по частоте между импульсами, несущими информацию $\delta\omega_{12} = |\omega_1 - \omega_2|$.

Сделаем численные оценки. При расстоянии между частотами $\delta\omega_{12} = |\omega_1 - \omega_2| \approx 10^9$ Гц, что представляет собой ширину линии не слишком хорошего полупроводникового лазера, и длительности короткого импульса в 1 пс ($\sigma_\infty \approx 10^{12}$ Гц), и типичном коэффициенте квадратичной дисперсии $\beta \approx 1\,\text{пс}^2/\text{км}$ [18] находим для допустимой длины линии

$$x_B \leq \frac{1}{10^9 \cdot 10^{12} \cdot (10^{-12})^2}\ [\text{км}] \approx 10^3\ \text{км},$$

для стандартных (далеких от рекордных) значений параметров.

Роль затухания сводится к двум эффектам. Из-за затухания в канале связи увеличивается доля измерений, в которых фотодетектор у пользователя B не сработал. Этот эффект снижает эффективность (долю нехолостых измерений), но не секретность. Второй эффект сводится к перенормировке дисперсии, рассмотренной выше. Ограничение на длину линии выглядит теперь следующим образом:

$$\frac{(1+\sigma_\infty^2\beta_{im}x)^2 + \beta_{re}^2 x^2 \sigma_\infty^4}{(1+\sigma_\infty^2\beta_{im}x)^2} \leq \frac{\sigma_\infty^2}{\delta\omega_{12}}, \tag{16}$$

при слабом затухании имеем

$$x_B \leq \frac{1}{\sqrt{\beta_{im}^2 + \beta_{re}^2}\,\delta\omega_{12}\sigma_\infty}, \tag{17}$$

где $\beta_{re}$ и $\beta_{im}$ – вещественная и мнимая части квадратичного коэффициента дисперсии.

В заключение выражаю благодарность С.В.Иорданскому, С.С.Назину и С.Т.Павлову за плодотворные обсуждения в процессе выполнения работы. Работа поддержана Российским фондом фундаментальных исследований (проект 96-02-19396).

---

1. M.E.Hellman, Sci. Amer. **241**, 130 (1979); G.J.Simmons, The Math. Intelligence **1**, 233 (1979).
2. C.E.Shannon, Bell Syst. Techn. J. 28, 657 (1949).
3. A.K.Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. C.Bennett, Phys. Rev. Lett. **68**, 3132 (1992).
5. C.H.Bennett, G.Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
6. A.K.Ekert, J.G.Rarity, P.R.Tapster, and G.M.Palma, Phys. Rev. Lett. **69**, 1293 (1992).
7. R.J.Hughes, D.M.Alde, P.Dyer et al., Contemporary Phys. **36**, 149 (1995).
8. S.J.D.Phoenix and P.D.Townsend, Contemporary Phys. **36**, 165 (1995).
9. C.Marand and P.D.Townsend, Optics Lett. **20**, 1695 (1995).
10. С.Н.Молотков, С.С.Назин, Письма в ЖЭТФ, **63**, 882 (1996).
11. C.H.Bennett, F.Bessette, G.Brassard et al., J. Cryptology **5**, 3 (1992).
12. J.D.Franson, Phys. Rev. **A45**, 3126 (1992).
13. J.Jeffers and S.Barnett, Phys. Rev. **A47**, 3291 (1993).
14. Л.И.Мандельштам, И.Е.Тамм, Известия АН СССР, сер. физ. **9**, N 1/2, 122 (1945).
15. Н.Бор, Избранные научные труды **2**, М.: Наука, 1971, с. 675.
16. Н.С.Крылов, В.А.Фок, ЖЭТФ **17**, 93 (1947); В.А.Фок, ЖЭТФ **42**, 1135 (1962).
17. В.В.Додонов, В.И.Манько, Труды ФИАН **183**, 52 (1987).
18. G.P.Argawal, *Nonlinear Fiber Optics*, ch. 3, 1989, Academic Press, Inc., Harcourt Brace Jovanovich, Publishers.