Письма в ЖЭТФ, том 64, вып.11, стр.813 - 816 © 1996г. 10 декабря

СУЩЕСТВУЕТ ЛИ ФУНДАМЕНТАЛЬНОЕ ОГРАНИЧЕНИЕ НА ДЛИНУ КАНАЛА СВЯЗИ В КВАНТОВОЙ КРИПТОСИСТЕМЕ НА ОДИНОЧНЫХ ФОТОНАХ?

С.Н.Молотков, С.С.Назин

Институт физики твердого тела РАН

142432 Черноголовка, Московская обл., Россия

Поступила в редакцию 15 октября 1996 г.

После переработки 5 ноября 1996 г.

Показано, что при произвольной дисперсии линии связи в отсутствие затухания в квантовой криптосистеме на одиночных фотонах нет формального ограничения на длину канала связи. Приведен рецепт нахождения формы сигнала, который обеспечивает сколь угодно малую суммарную длительность по времени сигнала на входе и выходе канала связи. Такой сигнал является в определенном смысле оптимальным.

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

Основная цель криптографии – секретная передача сообщений. Квантовая криптография гарантирует конфиденциальное распространение ключа (случайной последовательности нулей и единиц) между законными пользователями. Секретность (детектирование попыток подслушивания) обеспечивается законами квантовой механики [1–8].

В работе [8] была предложена квантовая криптосистема, основанная на использовании трех однофотонных сигналов. Два сигнала, несущие информацию о ключе, имеют хорошо определенные частоты ω_1 и ω_2, третий – короткий по времени сигнал (соответственно с широким частотным спектром) – используется для обнаружения возможных попыток подслушивания во время распространения ключа. Для обеспечения секретности системы нужно с достаточной точностью фиксировать моменты входа фотона в линию у пользователя A ($t(0)$) и его регистрации на другом конце линии пользователем B ($t(L)$, L – длина линии):

$$\Delta t(0), \Delta t(L) \ll \frac{1}{|\omega_1 - \omega_2|}. \qquad (1)$$

В реальных системах в качестве квантового канала связи используется оптоволоконная линия, имеющая частотную дисперсию. Поэтому эффективная длительность короткого сигнала на приемном конце $\Delta t(L)$, вообще говоря, увеличивается, что может накладывать ограничения (при заданных ω_1 и ω_2 и дисперсии) на длину линии. В связи с этим возникает естественный вопрос о том, какова должна быть спектральная и временная форма сигнала, при которой расплывание сигнала будет минимальным.

Данная задача решается вариационным методом, который впервые использовался Майером и Леонтовичем в 1934 г. [9] в задаче об определении спектра сигнала в радиотехнических системах, который минимизирует соотношение неопределенностей частота–время $\Delta\omega \cdot \Delta t$ (см. также обзор [10]).

Мы будем искать спектральную форму сигнала, при которой достигается минимум функционала

$$\Omega = \min\{[\Delta t(0)]^2 + [\Delta t(L)]^2\}. \qquad (2)$$

Пусть спектральная форма сигнала на входе в линию (при $x = 0$) задается функцией $g(\omega)$; тогда временна́я форма сигнала имеет вид

$$f(t, 0) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} g(\omega) \exp(-i\omega t) d\omega. \tag{3}$$

Сдвигом начала отсчета времени всегда можно добиться того, чтобы среднее время $t(0)$ входа фотона в линию было равно нулю:

$$\bar{t}(0) = \int_{-\infty}^{\infty} t|f(t, 0)|^2 dt = 0. \tag{4}$$

Ограничимся сначала рассмотрением вещественных четных по времени сигналов $f(t, 0)$; в этом случае спектральная функция $g(\omega)$ – вещественная и четная функция частоты.

Временная форма сигнала на приемном конце линии $x = L$ имеет вид

$$f(t, L) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} g(\omega) \exp(ik(\omega)L - i\omega t) d\omega, \tag{5}$$

где $k(\omega)$ – волновой вектор, который считаем вещественным (линия без затухания). Разброс времен регистрации фотона в точке $x = L$ дается соотношением

$$[\Delta t(L)]^2 = \int_{-\infty}^{\infty} (t - \bar{t}(L))^2 |f(t, L)|^2 dt, \tag{6}$$

где $\bar{t}(L)$ – среднее значение времени регистрации фотона на приемном конце линии в точке $x = L$, равное

$$\bar{t}(L) = \frac{\int_{-\infty}^{\infty} t|f(t, L)|^2 dt}{\int_{-\infty}^{\infty} |f(t, L)|^2 dt}. \tag{7}$$

Воспользовавшись тем обстоятельством, что преобразование Фурье переводит умножение на t в дифференциальный оператор $\frac{1}{i}\frac{d}{d\omega}$, легко проверить, что

$$\bar{t}(L) = L\langle k' \rangle, \tag{8}$$

где

$$\langle k' \rangle = \int_{-\infty}^{\infty} \frac{dk(\omega)}{d\omega} g^2(\omega) / \int_{-\infty}^{\infty} |f(t, L)|^2 dt. \tag{9}$$

Поскольку $\frac{dk(\omega)}{d\omega} = \frac{1}{v(\omega)}$ ($v(\omega)$ – групповая скорость), очевидно, что $\bar{t}(L)$ представляет собой среднее время долета пакета до точки L.

Функционал, подлежащий минимизации, с учетом нормировки сигнала,

$$\int_{-\infty}^{\infty} g^2(\omega) d\omega = 1, \tag{10}$$

принимает вид

$$\Omega = \min\{[\Delta t(0)]^2 + [\Delta t(L)]^2\} = \int_{-\infty}^{\infty} \left[2\left(\frac{dg(\omega)}{d\omega}\right)^2 + L^2 U(\omega) g^2(\omega) \right] d\omega, \tag{11}$$

где введено обозначение

$$U(\omega) = \left(\frac{dk(\omega)}{d\omega} - \langle k' \rangle \right)^2 . \tag{12}$$

Очевидно, что "потенциал" $U(\omega)$ всегда положителен, а при $\omega \to \infty$ он к тому же обращается в ноль, если $\langle k' \rangle = 1/c$ (при предельно больших частотах дисперсия отсутствует, $k(\omega) \to \omega/c$ при $\omega \to \infty$).

Заметим теперь, что формально функционал (11) с точностью до несущественных множителей совпадает с функционалом, соответствующим уравнению Шредингера с потенциалом $U(\omega) \geq 0$ и энергией λ^2.

$$-2\frac{d^2 g(\omega)}{d\omega^2} + L^2 U(\omega) g(\omega) = \lambda^2 g(\omega) \tag{13}$$

Исходя из этой аналогии легко показать, что соответствующим выбором функции $g(\omega)$ можно придать функционалу (11) любое сколь угодно малое положительное значение. Действительно, выбирая функцию $g(\omega)$ так, чтобы она была сосредоточена почти полностью в области больших ω, где дисперсия $k(\omega)$ уже несущественна, можно сделать $\langle k' \rangle$ сколь угодно близким к $1/c$. При этом потенциал $U(\omega)$ будет на бесконечности сколь угодно мал, а в таком потенциале есть волновые функции, отвечающие сколь угодно малой энергии частицы. Конкретно, выбирая $g(\omega) \propto \exp(-(\tau\omega)^2)$, можно сделать функционал (11) сколь угодно малым, устремляя τ к нулю (при этом $f(t,0)$ и $f(t,L)$ будут стремиться соответственно к $\delta(t)$ и $\delta(t - L/c)$).

Решение уравнения (13) дает функции непрерывного спектра, отвечающие энергии λ^2. Величина энергии (λ^2) в непрерывном спектре, и, соответственно, значение функционала (11), могут быть выбраны сколь угодно малыми. При данном λ решение уравнения (13) дает оптимальное решение. Оптимальное в том смысле, что ширина спектра сигнала по частоте, при выбранной суммарной длительности сигнала как на входе, так и на выходе из линии не превышающей λ, является наиболее узкой. Длительности импульса по времени на входе и на выходе из линии при этом примерно одинаковы.

Разумеется, всегда можно выбрать на входе достаточно короткий по времени (и, соответственно, широкий по частоте) сигнал, длительность которого на выходе не будет превышать выбранное λ. Однако при этом приходится гораздо сильнее "размазывать" входной сигнал по частоте, чем это реально требуется, если использовать оптимальное (в указанном выше смысле) решение.

В отсутствие дисперсии ($k(\omega) = \frac{\omega}{c}$, потенциал $U(\omega)$ обращается в нуль) решение вариационной задачи (11) сводится к решению уравнения

$$-2\frac{d^2 g(\omega)}{d\omega^2} = 0, \tag{14}$$

с граничным условием $\frac{dg(\omega)}{d\omega}\Big|_{\omega=0} = 0$. Решение последнего приводит к спектральной плотности $g(\omega) = const$, и временная форма импульса при этом принимает вид

$$f(t,0) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp(-i\omega t) d\omega = \delta(t), \tag{15}$$

и

$$f(t,L) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-i\left(\left(\frac{L}{c} - t\right)\omega\right) d\omega = \delta\left(t - \frac{L}{c}\right)\right). \tag{16}$$

Таким образом, формально, в отсутствие затухания при любой длине линии и любом законе дисперсии в ней можно подобрать форму сигнала таким образом, чтобы его эффективная размазка по времени как в точке $x = 0$, так и в точке $x = L$ были сколь угодно малы. Однако с физической точки зрения очевидно, что наличие затухания в линии в области высоких частот (именно в этой области сосредоточены сигналы, доставляющие функционалу (11) сколь угодно малые значения) может существенно изменить картину и привести к тому, что функционал (11) будет ограничен снизу некоторым положительным числом.

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

---

1. A.K.Ekert, Phys. Rev. Lett. **67**, 661 (1991).
2. C.Bennett, Phys. Rev. Lett. **68**, 3132 (1992).
3. C.H.Bennett, G.Brassard, N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
4. A.K.Ekert, J.G.Rarity, P.R.Tapster, G.M.Palma, Phys. Rev. Lett. **69**, 1293 (1992).
5. R.J.Hughes, D.M.Alde, P.Dyer, G.G.Luther, G.L.Morgan, M.Schauer, Contemporary Phys. **36**, 149 (1995).
6. S.J.D.Phoenix, P.D.Townsend, Contemporary Phys. **36**, 165 (1995).
7. C.Marand, P.D.Townsend, Optics Lett. **20**, 1695 (1995).
8. С.Н.Молотков, С.С.Назин, Письма в ЖЭТФ **63**, 882 (1996).
9. А.Г.Майер, Е.А.Леонтович, ДАН СССР **4**, 353 (1934).
10. В.В.Додонов, В.И.Манько, Труды ФИАН **183**, 52 (1987).