Письма в ЖЭТФ, том 80, вып. 7, с. 576 – 582 10 октября

К вопросу об обосновании квантовой криптографии на временных сдвигах

С. Н. Молотков

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

Факультет вычислительной математики и кибернетики, МГУ им. М. В. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 8 сентября 2004 г.

Представлено математическое обоснование секретности квантовой криптографии на временных сдвигах. Описаны процедуры приготовления и измерения наиболее сильно локализованных состояний с носителем в конечной частотной полосе. Показано, что измерений состояний в конечной частотной полосе и конечном временном окне достаточно для обнаружения *любых* изменений входных состояний. Кратко обсуждается использование существующих мультиплексных оптоволоконных систем на базе массива дифракционных решеток (AWG) для использования в квантовой криптографии на временных сдвигах.

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

В квантовой криптографии секретность ключа, по сути, гарантируется тем обстоятельством, что в квантовой механике невозможно точное одновременное измерение наблюдаемых, которым отвечают некоммутирующие операторы, что в определенном смысле является следствием фундаментального соотношения неопределенностей Гейзенберга [1 – 4].

Ранее были предложены системы квантовой криптографии на временных сдвигах [5]. Использование таких систем требует математического обоснования их секретности. Ниже будет показано, что квантовая криптография на паре неортогональных состояний (протокол B92 [2]) за счет временного сдвига на состояниях со спектром в конечной частотной полосе позволяет детектировать *любые* изменения состояний, что гарантирует их секретность. Привлекательность такой схемы состоит в том, что по структуре передаваемых состояний и их измерений, система потенциально наиболее близка к существующим классическим оптоволоконным системам и не требует специфических оптоволоконных компонентов в отличие, например, от систем с фазовым кодированием [6] и пассивной самокомпенсацией [7, 8].

Секретность квантовой криптографии на состояниях со спектром в конечной частотной полосе, где неортогональность (перекрытие) достигается за счет временных сдвигов состояний, тесно связана с фундаментальным соотношением неопределенностей энергия-время. Время является параметром, а не динамической переменной [9]. Данное обстоятельство накладывает специфические ограничения при использовании данного соотношения неопределенностей для целей квантовой криптографии [10].

Любая система квантовой криптографии включает процедуру приготовления состояний, а также процедуру их измерения. Любое измерение, если оно дает информацию об одном из неортогональных состояний, неизбежно приводит к его изменению [3]. С математической точки зрения измерение описывается некоторым разложением единицы в пространстве состояний, для достижения секретности принципиально важно, чтобы измерение было устроено таким образом, что оно гарантирует детектирование *любых* попыток подслушивания (*любых* изменений состояний). Обнаружение *любых* изменений состояний выражается в квантовой механике в том, что *любое* изменение должно приводить к изменению статистики результатов квантовомеханических измерений на приемном конце. На сегодняшний день существует несколько доказательств секретности квантовой криптографии на паре неортогональных состояний, в которых используются различные типы измерений [11 – 16].

Один из вариантов квантовой криптографии основан на использовании пары неортогональных состояний со спектром в конечной частотной полосе W и максимально локализованных во временном окне $(-T/2, T/2)$ (величина T при заданной W будет уточнена ниже). Пусть имеется пара однофотонных неортогональных состояний за счет сдвига по времени на величину τ_0, отвечающих 0 и 1 (далее $\hbar = c = 1$). Будем рассматривать состояния, распространяющиеся в одном направлении, волновой вектор $k > 0$.

$$|u_1\rangle = \int d\hat{x}\tilde{u}_1(\hat{x})a^+(\hat{x})|0\rangle,$$

$$a^+(\hat{x}) = \frac{1}{2\pi}\int d\hat{k}\delta(\hat{k}^2)\theta(k_0)e^{-i\hat{k}\hat{x}}a^+(k),$$
$$\hat{k}\hat{x} = kx - k_0 t, \quad \hat{k} = (k, k_0), \quad \hat{x} = (x, t); \tag{1}$$

далее,

$$|u_1\rangle = \int d\hat{k}\tilde{u}_1(\hat{k})\delta(\hat{k}^2)\theta(k_0)a^+(k)|0\rangle =$$
$$= \int \frac{dk}{k_0}\tilde{u}_1(k, k_0 = |k|)|k\rangle = \int\limits_W dk u_1(k)|k\rangle, \tag{2}$$

$$|k\rangle = a^+(k)|0\rangle, \quad \langle k|k'\rangle = k_0\delta(k - k'),$$
$$u_1(k) = \frac{\tilde{u}_1(k,k)}{\sqrt{k}}, \quad k_0 = k, \quad \tau = x - t. \tag{3}$$

Вклад в физическое состояние дают только те значения $\hat{k}$, которые лежат на массовой поверхности $k_0 = |k| = k$ $(k > 0)$. Аналогично для сдвинутого по времени состояния

$$|U(\tau_0)u_1\rangle = \int\limits_W dk e^{-ik\tau_0}u_1(k)a^+(k)|0\rangle =$$
$$= \int\limits_W dk e^{-ik\tau_0}u_1(k)|k\rangle. \tag{4}$$

Состояния неортогональны,

$$\langle U(\tau_0)u_1|u_1\rangle = \int\limits_W dk e^{ik\tau_0}|u_1(k)|^2, \tag{5}$$

если величина сдвига τ_0 меньше масштаба временной локализации состояния $\tau_0 < T \approx 1/W$.

Одно из измерений, которое чувствительно к любым изменениям состояний, описывается разложением единицы (например, [17]):

$$\mathcal{M}_0 = \frac{(I - |U(\tau_0)u_1\rangle\langle U(\tau_0)u_1|)}{1 + \langle U(\tau_0)u_1|u_1\rangle},$$
$$\mathcal{M}_1 = \frac{(I - |u_1\rangle\langle u_1|)}{1 + \langle U(\tau_0)u_1|u_1\rangle}, \tag{6}$$
$$\mathcal{M}_? = I - \mathcal{M}_0 - \mathcal{M}_1;$$

I – единичный оператор в пространстве состояний, натянутом на векторы $|u_1\rangle$ и $|U(\tau_0)u_1\rangle$. Пространство результатов на приемном конце состоит из трех событий: 0, 1, ?. Исходы 0 и 1 являются исходами с определенным результатом (conclusive). То есть срабатывание в канале $\mathcal{M}_0$ может быть лишь на состоянии $|U(\tau_0)u_1\rangle$ и никогда на входном состоянии $|u_1\rangle$, и наоборот. Отсчеты в канале $\mathcal{M}_?$ являются исходами с неопределенным результатом (inconclusive), поскольку могут иметь место как на состоянии $|u_1\rangle$, так и на состоянии $|U(\tau_0)u_1\rangle$. Измеряющие операторы в каналах 0 и 1 являются по сути (с точностью до нормировки) проекторами.

Пусть имеется состояние с носителем в частотной полосе W:

$$|\varphi\rangle = \int\limits_W dk\varphi(k)|k\rangle = \int\limits_{-\infty}^{\infty} d\tau\varphi(\tau)|\tau\rangle,$$
$$\varphi(\tau) = \frac{1}{2\pi}\int\limits_W dk e^{ik\tau}\varphi(k), \tag{7}$$
$$|\tau\rangle = \frac{1}{2\pi}\int\limits_W dk e^{-ik\tau}|k\rangle,$$

где $\varphi(\tau)$ – амплитуда состояния в пространственно-временном представлении и $\tau = x - t$. Отметим, что базисные состояния $|\tau\rangle$ в пространственно-временном представлении неортогональны в отличие от базисных состояний в импульсном представлении $|k\rangle$. Рассмотрим измерение, которое реализуется при помощи фильтра с частотной полосой W и "заслонки" (модулятора), которая открывается перед фотодетектором на временном окне $(-T/2, T/2)$. Такое измерение описывается разложением единицы в пространстве состояний с носителем в частотной полосе W:

$$I(W) = \int\limits_W dk|k\rangle\langle k| = \int\limits_{-\infty}^{\infty} d\tau|\tau\rangle\langle\tau| =$$
$$= \mathcal{M}(-T/2, T/2) + \mathcal{M}((-\infty,\infty)/(-T/2, T/2)), \tag{8}$$

$$\mathcal{M}(-T/2, T/2) = \int\limits_{-T/2}^{T/2} d\tau|\tau\rangle\langle\tau| =$$
$$= \int\limits_W\int\limits_W dk dk'\mathcal{K}(k - k', T)|k\rangle\langle k'|, \tag{9}$$

$$\mathcal{M}((-\infty,\infty)/(-T/2, T/2)) = I(W) - \mathcal{M}(-T/2, T/2), \tag{10}$$

где ядро

$$\mathcal{K}(k - k', T) = \frac{1}{\pi}\frac{\sin(k - k')T}{k - k'}. \tag{11}$$

Пространство результатов состоит из двух подмножеств – отсчетов во временном окне $(-T/2, T/2)$ и вне его $(-\infty,\infty)/(-T/2, T/2)$. Вероятность отсчетов для состояний во временном окне и "отфильтрованных" в частотную полосу W есть

$$\Pr(-T/2,T/2)=\mathrm{Tr}\{\mathcal{M}(-T/2,T/2)|\varphi\rangle\langle\varphi|\}= \int\limits_{-T/2}^{T/2} d\tau|\varphi(\tau)|^2. \quad (12)$$

Далее нас будут интересовать состояния с конечной частотной полосой, максимально локализованные во временном окне $(-T/2,T/2)$, то есть состояния, которые реализуют максимум функционала

$$\max_{\varphi}\left\{\frac{\int\limits_{-T/2}^{T/2} d\tau|\varphi(\tau)|^2}{\int\limits_{W} dk|\varphi(k)|^2}\right\}. \quad (13)$$

Амплитуда (волновая функция) таких состояний удовлетворяет интегральному уравнению, которое определяет специальные функции вытянутого сфероида (prolate spheroidal functions), возникающие в различных задачах математической физики (например, [18, 19]):

$$\lambda(WT)u_n(k)=\frac{1}{\pi}\int\limits_{W} dk\mathcal{K}(k-k',T)u_n(k'), \quad (14)$$

где собственные числа $\lambda_n(WT)$ образуют убывающую серию $1>\lambda_1(WT)>\lambda_2(WT)>\ldots>\lambda_n(WT)>\ldots 0$ $(n=1,\ldots\infty)$. Степень локализации (доля нормировки) во временном окне $(-T/2,T/2)$ $|u_n\rangle$ состояния равна n-му собственному числу:

$$\Pr(-T/2,T/2)=\mathrm{Tr}\{\mathcal{M}(-T/2,T/2)|u_n\rangle\langle u_n|\}= \int\limits_{-T/2}^{T/2} d\tau|u_n(\tau)|^2=\lambda_n(WT). \quad (15)$$

Степень локализации зависит лишь от произведения ширины частотной полосы на временное окно измерения, то есть от параметра WT (см. детали в [18]). Собственные числа обладают замечательным свойством [18, 20]. При фиксированном $WT\gg 1$ имеется $N=[WT]$ собственных чисел, собственные функции которых локализованы во временном окне с вероятностью, близкой к единице $(\lambda_n(WT)\approx 1)$, остальные собственные функции $(n>N)$ имеют долю нормировки во временном окне, близкую к нулю $(\lambda_n(WT)\approx 0)$, то есть основная нормировка набирается вне временного окна $(-T/2,T/2)$. Переходная область от собственных чисел с весом ≈ 1 к числам с весом ≈ 0 составляет $\ln(4\pi WT)$ [20]. Отметим также, что собственные функции имеют $n-1$ нулей в частотной полосе, это обстоятельство будет использовано ниже при приготовлении таких состояний.

Отметим также, что в базисе состояний $|u_n\rangle$ измеряющий оператор $\mathcal{M}(-T/2,T/2)$ диагонален:

$$\mathcal{M}(-T/2,T/2)=\sum_{n=1}^{\infty}\lambda_n(WT)|u_n\rangle\langle u_n|. \quad (16)$$

Также имеет место несложно проверяемая формула, которая нам потребуется далее:

$$\sqrt{\mathcal{M}(-T/2,T/2)}= \sqrt{\int\limits_{-T/2}^{T/2}\frac{d\tau}{2\pi}\left(\int\limits_{W}\frac{dk}{\sqrt{k}}\mathrm{e}^{-ik\tau}|k\rangle\right)\left(\int\limits_{W}\frac{dk'}{\sqrt{k'}}\mathrm{e}^{ik'\tau}\langle k'|\right)}= =\frac{1}{\pi}\int\limits_{0}^{\infty}\frac{d\zeta}{\zeta^{1/2}}\frac{\mathcal{M}(-T/2,T/2)}{(\zeta I(W)+\mathcal{M}(-T/2,T/2))}= =\sum_{n=1}^{\infty}\sqrt{\lambda_n(WT)}|u_n\rangle\langle u_n|, \quad (17)$$

Далее нас будет интересовать ситуация, когда $WT\approx 1$, то есть имеется одна наиболее сильно локализованная собственная функция $(\lambda_1(WT)\approx 1$, $\lambda_n(WT)\ll\lambda_1(WT)$ при $n>1)$.

Если удается приготовить состояние $|u_1\rangle$ с любой наперед заданной точностью, то измерения (16) в конечной частотной полосе и временном окне $(-T/2,T/2)$ достаточно, чтобы обнаружить *любые* изменения состояния, то есть никакие *другие* состояния не дадут ту же самую статистику результатов измерения. *Причем, приготовление и измерение состояний реализуется естественным образом при помощи стандартных оптоволоконных элементов. Роль затвора выполняет оптоволоконный модулятор, а роль частотного фильтра играет отдельный канал в мультиплексной системе на основе AWG – диффракционной решетки на массиве волноводов (Arrayed Waveguide Grating).*

Действительно, вероятность отсчетов в окне $(-T/2,T/2)$ на входном состоянии $|u_1\rangle$ есть

$$\Pr((-T/2,T/2))= \mathrm{Tr}\{\left(\sum_{n=1}^{\infty}\lambda_n(WT)|u_n\rangle\langle u_n|\right)|u_1\rangle\langle u_1|\}=\lambda_1(WT), \quad (18)$$

соответственно, вероятность отсчетов вне данного временного окна равна

$$\Pr((-\infty,\infty)/(-T/2,T/2))=1-\lambda_1(WT). \quad (19)$$

Покажем теперь, что любое другое состояние, отличное от $|u_1\rangle$, будет давать другую статистику отсчетов при измерении (16). *Для дальнейшего важно,*

что измерение устроено так, что измеряющий оператор во временном окне $(-T/2, T/2)$ *"проектирует" (пропускает) только такие состояния, носитель которых заключен в частотной полосе* W. Любое другое состояние в конечной частотной полосе может быть представлено разложением по базису состояний $|u_n\rangle$. Пусть модифицированное состояние есть

$$|\tilde{u}\rangle = a_1|u_1\rangle + \sum_{n\geq 2}^{\infty} a_n|u_n\rangle. \tag{20}$$

Условие нормировки требует, чтобы

$$|a_1|^2 + \sum_{n\geq 2}^{\infty} |a_n|^2 = 1. \tag{21}$$

Соответственно, вероятность отсчетов во временном окне измерения на данном входном состоянии равна

$$\Pr(-T/2, T/2)) =$$

$$= \mathrm{Tr}\{\left(\sum_{n=1}^{\infty} \lambda_n(WT)|u_n\rangle\langle u_n|\right)|\tilde{u}\rangle\langle\tilde{u}|\} =$$

$$= \lambda_1(WT)|a_1|^2 + \sum_{n\geq 2}^{\infty} \lambda_n(WT)|a_n|^2 < \lambda_1(WT), \tag{22}$$

и всегда меньше, чем вероятность отсчетов на входном состоянии $|u_1\rangle$. С учетом того, что состояние $|u_1\rangle$ с носителем в частотной полосе W является наиболее локализованным во временном окне измерения $(1 > \lambda_1(WT) \gg \lambda_n(WT),\ n \geq 2)$, имеем

$$|a_1|^2 = 1 - \sum_{n\geq 2}^{\infty} |a_n|^2,$$

$$\lambda_1(WT) - \lambda_1(WT)\left(\sum_{n\geq 2} |a_n|^2\right) +$$

$$+ \sum_{n\geq 2}^{\infty} \lambda_n(WT)|a_n|^2 < \lambda_1(WT). \tag{23}$$

Вообще говоря, достаточно только условия $\lambda_1(WT) > \lambda_n(WT)$ $(n \geq 2)$ и не требуется условие $\lambda_1(WT) \gg \gg \lambda_n(WT)$. Однако чем сильнее нарушение неравенства, тем легче детектировать изменения состояния.

Для квантовой криптографии временное окно $(-T/2, T/2)$ есть сумма двух временных окон (см. рис.1), в которых имеют место conclusive и inconclusive исходы. То есть измеряющий оператор представляется как сумма двух операторов, отнесенных к соответствующим окнам $T = T^{(0)}_{\mathrm{con}} + T_{\mathrm{incon}}$:

$$\mathcal{M}(-T/2, T/2) = \mathcal{M}_{\mathrm{con}}(-T/2, -T/2 + T^{(0)}) + \\ + \mathcal{M}_{\mathrm{incon}}(-T/2 + T^{(0)}, T/2). \tag{24}$$

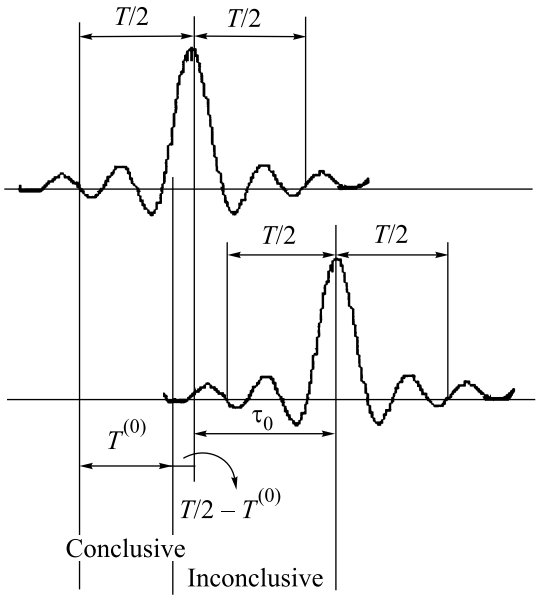

Рис.1

Вероятность получения conclusive исхода равна

$$\Pr^{OK}(T_{\mathrm{con}}) =$$

$$= \mathrm{Tr}\{\mathcal{M}_{\mathrm{con}}(-T/2, -T/2 + T^{(0)})|u_1\rangle\langle u_1|\} =$$

$$= \frac{\lambda_1(WT) - \lambda_1(W(T - 2T^{(0)}))}{2}, \tag{25}$$

и вероятность inconclusive исхода

$$\Pr^{OK}(T_{\mathrm{incon}}) =$$

$$= \mathrm{Tr}\{\mathcal{M}_{\mathrm{incon}}(-T/2 + T^{(0)}, T/2)|u_1\rangle\langle u_1|\} =$$

$$= \lambda_1(WT) - \Pr^{OK}(T_{\mathrm{con}}). \tag{26}$$

В окне T_{con} из-за "хвостов" состояния $|U(\tau_0)u_1\rangle$ могут быть отсчеты от этого состояния с вероятностью (см. рис.1)

$$\Pr^{\overline{OK}}(T^{(0)}_{\mathrm{con}}) =$$

$$\mathrm{Tr}\{\mathcal{M}_{\mathrm{con}}(-T/2, -T/2 + T^{(0)})|U(\tau_0)u_1\rangle\langle U(\tau_0)u_1|\} =$$

$$= \frac{1 - \lambda_1(2(\tau_0 + \frac{T}{2} - T^{(0)}))}{2}, \tag{27}$$

что является ошибкой, поэтому вероятность правильной идентификации состояния $|u_1\rangle$, отвечающего 0, если результат получен в окне $T^{(0)}_{\mathrm{con}}$, равна

$$p_0 = \frac{\Pr^{OK}(T^{(0)}_{\mathrm{con}})}{\Pr^{OK}(T^{(0)}_{\mathrm{con}}) + \Pr^{\overline{OK}}(T_{\mathrm{con}})} = \tag{28}$$

$$\frac{\lambda_1(WT)-\lambda_1(W(T-2T^{(0)}))}{\lambda_1(WT)-\lambda_1(W(T-2T^{(0)}))+1-\lambda_1(2(\tau_0+\frac{T}{2}-T^{(0)}))}.$$

Соответственно, вероятность ошибки при идентификации состояний при получении отсчета в окне conclusive

$$p_0^{\rm err}=1-p_0. \tag{29}$$

Данная ошибка имеет место даже в отсутствие подслушивателя и шума в канала и, очевидно, связана с тем, что состояния в конечной частотной полосе формально являются бесконечно протяженными, и всегда имеют место "хвосты", которые попадают в эту область. Отметим, что для измерений (6) в идеальном канале при получении conclusive результата состояния $|u_1\rangle$ или $|U(\tau_0)u_1\rangle$ идентифицируются с нулевой ошибкой, если имел место conclusive отсчет. Величину conclusive временного окна необходимо выбирать такой, чтобы ошибка идентификации была мала. Например, при $WT=2$ (см. численные данные для $\lambda_n(WT)$ в [18,20]), $\tau_0=T/2$ (перекрытие состояний за счет неортогональности при этом $\langle u_1|U(\tau_0)u_1\rangle\approx 0.5$) выбор conclusive временного окна $T^{(0)}=T/4$ дает для вероятности ошибки

$$\begin{aligned}
&{\rm Pr}^{OK}(T_{\rm con}^{(0)})=\frac{\lambda_1(WT)-\lambda_1(WT/2)}{2}=\\
&=\frac{0.8056-0.5725}{2}=0.15399,\\
&{\rm Pr}^{\overline{OK}}(T_{\rm con}^{(0)})=\frac{1-\lambda_1(3WT/2)}{2}=\\
&=\frac{1-0.99512}{2}=0.00244,\\
&p_0^{\rm err}=0.0156\approx 1.5\%.
\end{aligned} \tag{30}$$

Аналогично для состояния $|U(\tau_0)u_1\rangle$ при получении отсчетов в окне $T_{\rm con}^{(1)}$ для этого состояния.

Не нужно путать ошибку за счет "хвостов" состояний при отсчете во временном окне conclusive с ошибкой различения пары неортогональных состояний при помощи измерений (6).

Важно отметить, что оптический фильтр, пропускающий на фотодетектор только состояния с частотным спектром внутри W, принципиально необходим для обеспечения секретности протокола. В противном случае возможна простая атака, когда подслушиватель производит такие же измерения во временных окнах conclusive и inconclusive, как и на приемном конце, и если получен результат в окне inconclusive (см. рис.1), то подслушиватель перепосылает состояние с широким частотным спектром, локализованное во временном окне inconclusive. При такой атаке, в отсутствие оптического фильтра с полосой W, статистика результатов измерений на приемном конце не меняется. При наличии фильтра перед фотодетектором такое невозможно, поскольку в данной частотной полосе не существует более локализованных состояний, чем $|u_1\rangle$ ($|U(\tau_0)u_1\rangle$).

Аналогично может быть реализован протокол BB84 путем соответствующего выбора сдвинутых по времени состояний и временного окна измерения [5].

Наиболее простой способ приготовления состояния $|u_1\rangle$ состоит в "вырезании" при помощи модулятора (оптического затвора) из состояния с узким частотным спектром $\delta W\ll W$ "части" состояния посредством открывания затвора на время $(-T/2,T/2)$ и пропускания через фильтр с частотной полосой W.

Покажем теперь, что процедура приготовления описывается операторами $\sqrt{\mathcal{M}(-T/2,T/2)}$, которые рассматриваются как элементы супероператора в разложении Крауса для него.

Действительно, действие оптического модулятора (затвора) сводится к тому, что при его открытии на определенный интервал времени на его выходе возникает состояние, которое локализовано лишь в этом временном интервале. То есть при измерении после модулятора этого состояния отсчеты будут иметь место только в данном временном интервале. Рассмотрим супероператор $\mathbf{T}[...]$, одним из элементов в разложении которого есть

$$\begin{aligned}
&\mathbf{T}[...]=\\
&=\sqrt{\mathcal{M}_{W_m}(-T/2,T/2)}[...]\sqrt{\mathcal{M}_{W_m}(-T/2,T/2)^{+}}+\\
&+\sqrt{I(W_m)-\mathcal{M}_{W_m}(-T/2,T/2)}[...]\\
&[...]\sqrt{I(W_m)-\mathcal{M}_{W_m}(-T/2,T/2)^{+}},
\end{aligned} \tag{31}$$

$$\begin{aligned}
&\mathcal{M}_{W_m}(-T/2,T/2)=\\
&\int\limits_{-T/2}^{T/2}\frac{d\tau}{2\pi}\left(\int\limits_{W_m}\frac{dk}{\sqrt{k}}e^{-ik\tau}|k\rangle\right)\left(\int\limits_{W_m}\frac{dk'}{\sqrt{k'}}e^{ik'\tau}\langle k'|\right)=\\
&=\sum_{n=1}^{\infty}\lambda_n(W_mT)|u_n(W_m)\rangle\langle u_n(W_m)|,
\end{aligned} \tag{32}$$

где $|u_n(W_m)\rangle$ – собственные функции интегрального уравнения (14) с W_m. Здесь W_m – полоса пропускания модулятора (затвора), которая должна быть достаточно широкой ($W_m\gg W\sim 1/T$). В этом случае

при любом входном состоянии $|\varphi\rangle$ с носителем в полосе $\delta W \ll W_m$ на выходе будет состояние, которое с вероятностью, сколь угодно близкой к единице, локализовано во временном окне $(-T/2, T/2)$, что следует из (32), поскольку $W_m T \gg 1$. Супероператор "вырезает" из состояния $|\varphi\rangle$ ту "часть", которая локализована в окне $(-T/2, T/2)$. При этом частотный спектр состояния эффективно "расширяется", оказывается $\sim W_m$. Дальнейшее пропускание через фильтр с частотной полосой W приводит к тому, что с подавляющей вероятностью на выходе оказывается состояние $|u_1\rangle$. Пропускание через фильтр приводит также к некоторой временной "размазке" состояния (в меру параметра WT). Действие фильтра описывается проектором $\mathcal{P}_W = \int\limits_W dk|k\rangle\langle k|$ к состоянию на выходе затвора. Действительно,

$$\frac{1}{\mathrm{Tr}\{\mathcal{P}_W \mathcal{M}_{W_m}(-T/2,T/2)\mathcal{P}_W|\varphi\rangle\langle\varphi|\}}\mathcal{P}_W \times$$
$$\times \left(\sqrt{\mathcal{M}_{W_m}(-T/2,T/2)}[|\varphi\rangle\langle\varphi|]\times\right.$$
$$\left.\times\sqrt{\mathcal{M}_{W_m}(-T/2,T/2))^+}\right)\mathcal{P}_W =$$
$$= \frac{1}{\mathrm{Tr}\{\mathcal{M}(-T/2,T/2)|\varphi\rangle\langle\varphi|\}} \times$$
$$\times \sqrt{\mathcal{M}(-T/2,T/2)}[|\varphi\rangle\langle\varphi|]\sqrt{\mathcal{M}(-T/2,T/2)^+}. \quad (33)$$

Далее, с учетом (31)–(32), видим, что если на входе было состояние $|\varphi\rangle$, то на выходе оптического затвора с фильтром будет состояние

$$|\varphi\rangle = \int\limits_{\delta W} dk\varphi(k)|k\rangle \to \frac{\sum_{n=1}^{\infty}\sqrt{\lambda_n(WT)}|u_n\rangle\overline{u}_n(0)}{\sqrt{\sum_{n=1}^{\infty}\lambda_n(WT)|\overline{u}_n(0)|^2}}. \quad (34)$$

Здесь введены обозначения $\overline{u}_n(0) = \int\limits_{\delta W} dk\varphi^*(k)u_n(k) \approx \approx \varphi^*(0)u_n(0)$, при $\delta W \ll W$. Мы сдвинули начало отсчета на центральную частоту $0 \leftrightarrow W_c$, W_c – центральная частота. Далее удобно выбрать, чтобы частотная полоса входного, почти монохроматического и, соответственно, протяженного в пространстве-времени состояния совпадала с центральной частотой фильтра, что обычно и бывает в оптоволоконных системах. В качестве источника может быть использован CW-лазер с узкой частотной полосой.

Воспользуемся теперь свойствами собственных чисел интегрального уравнения (14). Например, если параметр $WT = 2$, то преобладающим является первое собственное число $\lambda_1(WT) = 0.88056$, $\lambda_2(WT) = 0.35564$, $\lambda_3(WT) = 0.035868...\lambda_8(WT) = 2.7 \cdot 10^{-14}$ (см. [18–20]). Напомним, что собственные функции $u_n(k)$ имеют $n-1$ нулей. Поэтому $\overline{u}_1(0) \neq 0$, $\overline{u}_2(0) \approx 0$, $\overline{u}_3(0) \ll \overline{u}_1(0)$. При значении параметра $WT = 2$ имеем состояние

$$\approx \frac{\sqrt{\tilde{\lambda}_1(WT)}|u_1\rangle + \sqrt{\tilde{\lambda}_3(WT)}|u_3\rangle}{\sqrt{\tilde{\lambda}_1(WT) + \tilde{\lambda}_3(WT)}}, \quad (35)$$

где $\tilde{\lambda}_n(WT) = \lambda_n(WT)|\overline{u}_n(0)|^2$. Однократное применение оптического затвора и фильтра с полосой W к "монохроматическому" состоянию с узким частотным спектром $\delta W \ll W$ дает на выходе состояние $|u_1\rangle$ с примесью других состояний не более 10^{-3}, так как $|\overline{u}_1(0)/\overline{u}_3(0)|^2 \approx 3.5 \cdot 10^{-2}$, и $\lambda_1(2)/\lambda_3(2) = 0.18$, соответственно, $\tilde{\lambda}_1(2)/\tilde{\lambda}_3(2) \approx 6 \cdot 10^{-3}$. В принципе, последовательное применение такой процедуры N раз уменьшает примесь других состояний экспоненциально быстро по параметру $(\tilde{\lambda}_3(WT)/\tilde{\lambda}_1(WT))^N$. В реальном эксперименте уже достаточно однократного применения.

Таким образом, оптический затвор с фильтром позволяют приготовить состояния, наиболее сильно локализованные в данном временном окне, путем "вырезания" из состояний с узким частотным спектром, получаемых, например, на выходе CW-лазера. В качестве фильтра может быть использована оптоволоконная система фильтров на основе AWG технологии, которая является стандартным элементом оптоволоконных систем передачи информации, работающих в мультиплексном режиме. Единственным требованием. которое должно быть соблюдено, – это условие, чтобы длительность импульсов T на выходе модулятора была согласована с частотной полосой W отдельного канала в системе фильтров AWG, в том смысле, чтобы было $WT \approx 1 \div 2$.

Здесь была решена только первая часть задачи по исследованию квантовой криптографии на временных сдвигах, показано, что измерения в конечной частотной полосе и конечном временном окне позволяют обнаруживать любые изменения входных состояний. Полный криптоанализ должен установить связь между изменением статистики результатов измерений и максимально возможной утечкой информации при таком изменении, что требует отдельного изложения.

Приведем некоторые численные оценки. Стандартно используемые оптоволоконные мультиплексные системы с частотой передачи[1)] 2.5 ГГц используют фильтры на базе AWG с шириной частотной полосы 0.02 нм. Такая система фильтров может быть

[1)] На сегодняшний день существуют оптоволоконные системы передачи с частотой в диапазоне ТГц. В этом случае точность стробирования лавинного фотодетектора должна составлять несколько пикосекунд.

использована для систем квантовой криптографии, при этом длительность импульсов по времени для соблюдения условия $WT \approx 2$ должна быть $T \approx$ ≈ 800 пс. Точность стробирования при этом должна быть ~ 100 пс. Однако это не означает, что ключ можно передавать с такой скоростью. Скорость передачи в системах квантовой криптографии лимитируется временем восстановления лавинного фотодетектора при счете фотонов. Важно, что существующие стандартные системы фильтров на базе AWG могут быть использованы для целей квантовой криптографии. Ширина частотных каналов фильтров диктует лишь длительность импульсов, частота же следования импульсов из-за медленного восстановления лавинного фотодетектора обычно составляет $\sim$ МГц.

Работа поддержана Академией Криптографии РФ, Российским фондом фундаментальных исследований (проект # 02-02-16289), а также междисциплинарным проектом МГУ.

1. S. Wiesner, SIGACT News **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, *Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India, December 1984, p. 175.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
4. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
5. С. Н. Молотков, Письма в ЖЭТФ **79**, 691 (2004).
6. C. Elliot, D. Pearson, and G.Troxel, quant-ph/0307049.
7. D. S. Bethune and W. P. Risk, New J. of Phys. **4**, 42.1 (2002).
8. D. S. Bethune, M. Navarro, and W. P. Risk, quant-ph/0104089.
9. A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, 1980.
10. С. Н. Молотков, Письма в ЖЭТФ **74**, 477 (2001).
11. A. K. Ekert, B. Huttner, G. M. Palma, and A.Peres, Phys. Rev. **A50**, 1047 (1994).
12. H. E. Brandt, J. M. Myer, and S. J. Lomonaco Jr., Phys. Rev. **A56**,4456 (1997).
13. B. A. Slutsky, R. Rao, Pang-Chen Sun, and Y. Fainman, Phys. Rev. **A57**, 2383 (1998).
14. K. Tamaki, M. Koashi, and N. Imoto, /quant-ph/0212161.
15. K. Tamaki, M. Koashi, and N. Imoto, /quant-ph/0212162.
16. K. Tamaki and N. Lutkenhaus, /quant-ph/0308048.
17. A. Peres, *Quantum Theory: Cocepts and Methods*, Kluwer, Dordrecht, 1993.
18. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **XL**, 40 (1961).
19. W. H. Fuchs, J. of Mathematical Analysis and Appl. **9**, 317 (1964).
20. D. Slepian, J. Math. and Phys., **44**, 99 (1965).