*ЖЭТФ, 1998, том 114, вып. 2(8), стр. 526–537* ©1998

# КВАНТОВАЯ КРИПТОГРАФИЯ НА «ЧАСТОТНЫХ» СОСТОЯНИЯХ ФОТОНА (ПРИМЕР ВОЗМОЖНОЙ РЕАЛИЗАЦИИ)

*С. Н. Молотков**

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

Поступила в редакцию 27 января 1998 г.

Предлагается квантовая криптосистема, использующая в качестве носителей информации однофотонные состояния с различным частотным спектром. Обсуждается возможная экспериментальная реализация криптосистемы.

## 1. ВВЕДЕНИЕ

Идея квантовой криптографии впервые была высказана в первоначально недоступной работе [1]. В современном виде протокол распространения ключа (секретной случайной последовательности нулей и единиц) был предложен в работе [2]. Новый качественный скачок в понимании секретности в квантовой криптографии возник после работ [3], в которых был предложен протокол обмена на неортогональных состояниях, и работы [4], где был описан протокол на эффекте Эйнштейна–Подольского–Розена.

Впоследствии были предложены различные варианты криптосистем, использующие как неортогональные состояния, так и эффект Эйнштейна–Подольского–Розена [5–22]. Были реализованы экспериментальные прототипы квантовых криптосистем, использующие для кодирования неортогональные состояния поляризации фотонов [5, 11, 12], а также принцип фазового кодирования на базе оптоволоконного интерферометра Маха–Цендера с разделением времени [8–10, 19] (усовершенствованный вариант схемы из работы [10] осуществлен в работе [19]). Наиболее длинный канал связи в квантовой криптографии, реализованный в лабораторных условиях, составляет 30 км [10]. Была продемонстрирована работа прототипа квантовой криптосистемы в естественных условиях с оптоволоконным кабелем длиной 23 км, проложенным под Женевским озером [18], а также между различными зданиями в лаборатории Лос-Аламоса [13].

Большинство упомянутых систем используют интерференционный принцип, который, грубо говоря, сводится к «расщеплению» фотона на передающем конце линии, и «собиранию» его на приемном конце. В данной работе предлагается квантовая криптосистема на различных частотных состояниях фотона, которая использует «внутреннюю интерференцию» различных частотных составляющих фотона. Возможно, подобная система может оказаться более устойчивой в работе, чем прямые интерференционные схе-

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

мы, хотя окончательный ответ может быть получен только при экспериментальной реализации.

Секретность ключа в квантовой криптографии основывается на двух фактах: 1) невозможности копирования (клонирования) заранее неизвестного квантового состояния [23]; 2) невозможности извлечения информации о квантовых состояниях без их возмущения, если они принадлежат неортогональному базису [3]. Формально в качестве носителей информации может быть использована любая пара неортогональных состояний, отвечающая логическим 0 и 1. Процедура детектирования (квантовомеханического измерения) на приемном конце должна быть устроена так, чтобы обнаруживать по результатам измерений любые попытки вторжения в канал связи — изменения состояний. Если в качестве носителей используется пара неортогональных состояний, $|\psi_0\rangle$ и $|\psi_1\rangle$, то формальные измерения даются проекторами [3]

$$\overline{E}_0 = 1 - |\psi_0\rangle\langle\psi_0|, \quad \overline{E}_1 = 1 - |\psi_1\rangle\langle\psi_1|,$$

действие которых сводится к проектированию на подпространства состояний, ортогональные соответственно векторам $|\psi_0\rangle$ и $|\psi_1\rangle$ [3]. Результат действия проекторов рассматривается как утверждение, и вероятность результата измерения дается выражениями:

$$\begin{aligned} &\mathrm{Pr} = \mathrm{Tr}\{\hat{\rho}_0\overline{E}_0\} = \mathrm{Tr}\{\hat{\rho}_1\overline{E}_1\} \equiv 0, \\ &\mathrm{Pr} = \mathrm{Tr}\{\hat{\rho}_0\overline{E}_1\} = \mathrm{Tr}\{\hat{\rho}_1\overline{E}_0\} = 1 - |\langle\psi_0|\psi_1\rangle|^2 \neq 0. \end{aligned} \tag{1}$$

Измерения при помощи $\overline{E}_0$ и $\overline{E}_1$ при идеальном канале связи (канале без шума) позволяют детектировать любые попытки подслушивания — изменения состояний. Первый ненулевой исход контрольного измерения однозначно указывает на присутствие подслушивателя. Действительно, когда известно, что был послан сигнал, например $|\psi_0\rangle$, измерения проводились при помощи $\overline{E}_0$ и получен ненулевой результат, то ненулевой результат рассматривается как утверждение того, что состояние $|\psi_0\rangle$ имеет ненулевую компоненту в соответствующем ортогональном дополнении гильбертова пространства (т. е. что состояние $|\psi_0\rangle$ было изменено).

Для реальных оптоволоконных каналов связи в качестве носителей информации используются фотонные состояния. Формально можно использовать любую пару неортогональных состояний фотонов (даже не обязательно однофотонных). Однако неясно, как реализовать экспериментально измерительную процедуру, отвечающую проекторам $\overline{E}_{0,1}$ для данной пары состояний. Проще всего было бы использовать пару неортогональных поляризаций, но оптоволокно не «держит» поляризацию (см. детали, например, в [11, 12]). В упомянутых прототипах квантовых криптосистем используется принцип фазового кодирования на базе интерферометров с разделением времени [8–10]. Через несколько минут работы интерферометра требуется дополнительная юстировка системы [10].

## 2. КРИПТОГРАФИЯ НА «ЧАСТОТНЫХ» СОСТОЯНИЯХ ФОТОНА

Ранее была предложена схема квантовой криптографии на эффекте Эйнштейна–Подольского–Розена для бифотонного поля [20]. Данная работа является развитием

идеи работы [20]. Ниже предлагается использовать частотные состояния, не использующие интерференцию на больших расстояниях.

Рассмотрим сначала формальную схему, а затем обсудим экспериментальную реализацию. В качестве носителей используются три однофотонных состояния: два информационных, отвечающих логическим нулю и единице, и одно контрольное состояние. Информационные состояния ортогональны друг другу. Контрольное состояние попарно неортогонально информационным. Использование только двух информационных состояний недостаточно для секретности, поскольку они достоверно различимы из-за их ортогональности друг другу.

Информационные состояния представляют собой чистые стационарные состояния с матрицами плотности

$$\hat{\rho}_0 = |e_0\rangle\langle e_0|, \quad \hat{\rho}_1 = |e_1\rangle\langle e_1|, \quad \langle e_1|e_0\rangle = 0, \tag{2}$$

где $|e_0\rangle$ и $|e_1\rangle$ — некоторые базисные состояния, относящиеся соответственно к энергиям $\omega_0$ и $\omega_1$. Контрольное состояние является нестационарным и содержит обе базисные компоненты, $|e_0\rangle$ и $|e_1\rangle$:

$$\begin{aligned} &|\psi_c(t_0)\rangle = \mathrm{e}^{-i\omega_0 t_0} f_0|e_0\rangle + \mathrm{e}^{-i\omega_1 t_0} f_1|e_1\rangle, \\ &\hat{\rho}_c(t_0) = |\psi_c(t_0)\rangle\langle\psi_c(t_0)|, \end{aligned} \tag{3}$$

и условие нормировки

$$|f_0|^2 + |f_1|^2 = 1.$$

Момент $t_0$ описывает начало отсчета времени — момент приготовления состояния (см. ниже). Матрица плотности в моменты $t > t_0$ получается подстановкой в аргумент $\hat{\rho}_c(t) = |\psi_c(t-t_0)\rangle\langle\psi_c(t-t_0)|$. Введение двух ортогональных информационных состояний уменьшает число «холостых» исходов из-за их различимости, если в процессе обмена не обнаружен факт подслушивания.

В данной схеме используются два типа измерений. Измерения частотного спектра описываются ортогональным разложением единицы в пространстве, натянутом на состояния $|e_0\rangle$, $|e_1\rangle$:

$$E_0 + E_1 = I, \quad E_0 = |e_0\rangle\langle e_0|, \quad E_1 = |e_1\rangle\langle e_1|, \tag{4}$$

где $I$ — единичный оператор. Второе семейство измерений связано с измерением времени и дается неортогональным разложением единицы (см., например, [24]), которое в нашем случае имеет вид

$$\begin{aligned} &\int_0^T E(dt) = I, \quad T = \frac{2\pi}{|\omega_1 - \omega_0|}, \\ &E(dt) = \left(\mathrm{e}^{-i\omega_0 t}|e_0\rangle + \mathrm{e}^{-i\omega_1 t}|e_1\rangle\right)\left(\langle e_0|\mathrm{e}^{i\omega_0 t} + \langle e_1|\mathrm{e}^{i\omega_1 t}\right)\frac{dt}{T}. \end{aligned} \tag{5}$$

Согласно общей идеологии квантовомеханических измерений, измерения проводятся в определенный момент времени [24–26]. Вероятность исхода измерений при помощи проекторов $E_0$ и $E_1$ не зависит от времени и равна

$$\begin{aligned} &\Pr = \mathrm{Tr}\{\hat{\rho}_0 E_0\} = 1, \quad \Pr = \mathrm{Tr}\{\hat{\rho}_1 E_1\} = 1, \quad \Pr = \mathrm{Tr}\{\hat{\rho}_{0,1} E_{1,0}\} \equiv 0, \\ &\Pr = \mathrm{Tr}\{\hat{\rho}_c(t) E_0\} = |f_0|^2, \quad \Pr = \mathrm{Tr}\{\hat{\rho}_c(t) E_1\} = |f_1|^2. \end{aligned} \tag{6}$$

Измерение времени дает распределение вероятностей исходов в интервале $(t, t + dt)$:

$$\Pr(dt) = \mathrm{Tr}\{\hat{\rho}_{0,1} E(dt)\} = 1 \cdot \frac{dt}{T}, \tag{7}$$

$$\begin{aligned} \Pr(dt) = \mathrm{Tr}\{\hat{\rho}_c(t) E(dt)\} &= |f_0 \exp[-i\omega_0(t - t_0)] + f_1 \exp[-i\omega_1(t - t_0)]|^2 \left(\frac{dt}{T}\right) = \\ &= \left\{1 + 2\mathrm{Re}\left[f_0 f_1^* \exp[-i(\omega_0 - \omega_1)(t - t_0)]\right]\right\} \left(\frac{dt}{T}\right). \end{aligned} \tag{8}$$

Для контрольного состояния вероятность представляет собой осциллирующую функцию с периодом $T = 2\pi/|\omega_1 - \omega_0|$. Данный набор измерений позволяет полностью восстанавливать информацию о состояниях — никакие другие матрицы плотности не воспроизводят статистики измерений, что позволяет детектировать любые попытки подслушивания (см. подробнее [22]).

Протокол генерации ключа выглядит следующим образом. Считается, что все параметры состояний известны всем, включая возможного подслушивателя. Пользователь *A* посылает в канал связи случайным образом состояния $\hat{\rho}_c$, $\hat{\rho}_0$ или $\hat{\rho}_1$. Пользователь *B* случайно и независимо от *A* выбирает тип измерения $E_0$, $E_1$ или $E(dt)$. После проведения серии измерений пользователь *A* для части измерений через открытый (доступный всем, включая подслушивателя) канал связи сообщает номера тех измерений, когда были посланы $\hat{\rho}_0$ и $\hat{\rho}_1$, и все номера, когда посылалось контрольное состояние $\hat{\rho}_c$. Пользователь *B* сортирует измерения в три группы в соответствии с тем, когда были посланы $\hat{\rho}_c$, $\hat{\rho}_0$ или $\hat{\rho}_1$. В каждой из этих трех групп выделяются три подгруппы в соответствии с измерительными процедурами $E_0$, $E_1$ или $E(dt)$. Например, для части посылок, когда пользователь *A* передавал состояние $\hat{\rho}_c$, относительная доля исходов измерений, когда использовались проекторы $E_0$ и $E_1$, должна составлять $|f_0|^2/|f_1|^2$ независимо от момента измерения. Для измерения $E(dt)$ вероятность результатов измерений в различные моменты времени должна сходиться к распределению вероятностей (8). Сходимость функции распределения по конечной выборке может быть проверена при помощи того или иного статистического критерия, например, критерия Колмогорова [27] (см. также [22]). Аналогично проверяется сходимость для измерений, когда посылались состояния $\hat{\rho}_0$ или $\hat{\rho}_1$. Например, для состояния $\hat{\rho}_0$ измерения при помощи $E_0$ должны давать во всех попытках одинаковый исход, не зависящий от момента измерения. При измерении $E_1$ во всех попытках независимо от момента измерения должен быть нулевой исход. Для измерения $E(dt)$ вероятность исхода определяется лишь длительностью интервала по времени $dt$ и не зависит от самого момента $t$.

Секретность протокола гарантируется неортогональностью информационных состояний контрольному и тем обстоятельством, что набор измерений является информационно полным, что позволяет детектировать любые попытки подслушивания — изменения состояний. Иначе говоря, никакие другие матрицы плотности не воспроизводят статистику измерений на приемном конце (подробнее см. [22]).

После того как установлен факт отсутствия подслушивания, пользователь *A* сообщает номера тех измерений, когда посылалось контрольное состояние. Все холостые

измерения, когда не было срабатывания детектора, отбрасываются. Далее, для оставшихся номеров пользователь *B* сообщает лишь номера тех измерений, в которых он использовал $E_0$ или $E_1$, но не сообщает, какое измерение, $E_0$ или $E_1$, использовалось в каждой конкретной попытке (эта информация известна теперь лишь *A* и *B*). Эти оставшиеся измерения дают секретный ключ (идентичную у пользователей *A* и *B* случайную последовательность нулей и единиц).

Проиллюстрируем, почему подслушиватель неизбежно будет ошибаться. Для получения информации о ключе подслушиватель должен отличать состояния $\hat{\rho}_0$ и $\hat{\rho}_1$. Для этого он должен проводить измерения узкополосным детектором (измерения $E_0$ или $E_1$). Если бы не было контрольного состояния $\hat{\rho}_c$, в котором присутствуют обе спектральные компоненты с частотами $\omega_0$ и $\omega_1$, то из-за взаимной ортогональности информационных состояний можно было бы однозначно определить, какое состояние присутствует в линии. Но их неортогональность контрольному состоянию будет неизбежно приводить к ошибкам, поскольку всегда будут измерения с неопределенным результатом. Например, если в линии присутствует $\hat{\rho}_c$, а подслушивателем проводилось измерение, например $E_0$, и получен ненулевой результат, то невозможно сделать однозначного заключения о том, какое состояние дало этот результат, $\hat{\rho}_c$ или $\hat{\rho}_0$. Перепосылка $\hat{\rho}_0$ вместо истинного $\hat{\rho}_c$ приведет к изменению статистики измерений у пользователя *B*. Узнать в одном измерении, что в состоянии одновременно присутствуют обе спектральные компоненты с энергиями $\omega_0$ и $\omega_1$ также невозможно из-за ортогональности компонент, поскольку для этого необходимо проводить измерения посредством $E_0E_1$. Такой проектор можно рассматривать как утверждение, что одновременно имеют место свойство $E_0$ (присутствует $\omega_0$) и $E_1$ (присутствует $\omega_1$). Однако из-за ортогональности ($E_0 \bigcap E_1 = \varnothing$) действие $E_0E_1$ на любой матрице плотности имеет тождественно нулевой результат. Нельзя также получить однозначную информацию об одновременном присутствии спектральных компонент при помощи более общих (не фон-неймановских) измерений, что гарантируется теоремой из [3].

## 3. ВОЗМОЖНАЯ РЕАЛИЗАЦИЯ КРИПТОСИСТЕМЫ

Обсудим теперь возможность экспериментальной реализации. В качестве носителей используются три однофотонных состояния вида

$$\begin{aligned} &|1_{\omega_0}\rangle = a^+_{\epsilon,\omega_0}|0\rangle, \quad |1_{\omega_1}\rangle = a^+_{\epsilon,\omega_1}|0\rangle, \\ &|1_c\rangle = f_0 e^{-i\omega_0 t_0} a^+_{\epsilon,\omega_0}|0\rangle + f_1 e^{-i\omega_1 t_0} a^+_{\epsilon,\omega_1}|0\rangle \end{aligned} \tag{9}$$

с соответствующими матрицами плотности

$$\hat{\rho}_{0,1} = |1_{\omega_{0,1}}\rangle\langle 1_{\omega_{0,1}}|, \quad \hat{\rho}_c = |1_c\rangle\langle 1_c|,$$

где $a^+_{\epsilon,\omega_i}$ — оператор рождения фоковского монохроматического состояния с частотой $\omega_i$ ($i = 0, 1$) и поляризацией $\epsilon$, $|0\rangle$ — вакуумное состояние. Разумеется, что строго монохроматические состояния являются идеализацией. Однако нет никаких принципиальных запретов на получение состояний, сколь угодно близких к монохроматическим.

Описанные выше процедуры измерений могут быть реализованы при помощи быстрого (достаточно широкополосного) фотодетектора, работающего в режиме ожидания,

и двух узкополосных фильтров на частотах $\omega_0$ и $\omega_1$. Согласно стандартной теории фотодетектирования [28], вероятность детектирования пропорциональна корреляционной функции поля первого порядка

$$\Gamma^{(1)}(t) = \mathrm{Tr}\left\{\hat{\rho}_i \hat{E}^{(-)}(x,t)\hat{E}^{(+)}(x,t)\right\}, \tag{10}$$

где

$$\hat{E}^{(+)}(x,t) = i\sum_{\omega_n}\sqrt{\frac{\hbar\omega_n}{2V}}a_{\epsilon_n,\omega_n}\exp(-i\omega_n t + ik_n x),$$

$$\hat{E}^{(-)}(x,t) = -i\sum_{\omega_n}\sqrt{\frac{\hbar\omega_n}{2V}}a^{+}_{\epsilon_n,\omega_n}\exp(i\omega_n t - ik_n x),$$

$V$ — нормировочный объем. На данном этапе удобнее использовать формальную нормировку состояний в конечном объеме (см. ниже). Можно даже использовать ненормированные состояния. При таком определении вероятности исходов измерений также будут ненормированными, но поскольку важна лишь относительная вероятность при разных измерениях, то ненормированность несущественна.

Измерения корреляционной функции поля (мгновенной интенсивности) $\Gamma^{(1)}(t)$ являются реализацией описанных выше измерений $E_{0,1}$ и $E(dt)$ в том смысле, что статистика исходов дает такую же информацию о состояниях, как и статистика измерений $E_{0,1}$ и $E(dt)$. Комбинация измерений при помощи быстрого фотодетектора и измерений с двумя узкополосными фильтрами и тем же фотодетектором позволяет получить информацию об амплитуде $|f_{0,1}|$ и об относительной фазе компонент $f_0$ и $f_1$, что исчерпывает информацию о состояниях (см. также [22]).

Вероятность $p$ зарегистрировать фотон в интервале времени $(t, t+dt)$ идеальным фотодетектором пропорциональна интенсивности поля $I(t) \propto \Gamma^{(1)}(t)$ [28]:

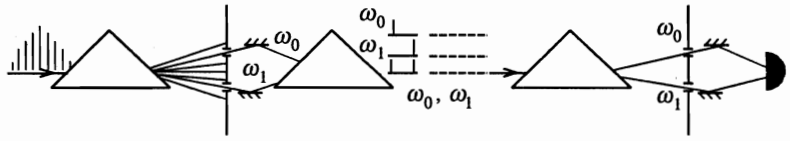
$$p(t)dt \propto I(t)dt = \Gamma^{(1)}(t)dt. \tag{11}$$

Если время срабатывания фотодетектора $\tau_{det} \ll 1/|\omega_1 - \omega_0|$, то такой фотодетектор реализует измерение $E(dt)$ в упомянутом выше смысле. Действительно, как видно из уравнения (10), для состояния (9) вероятность регистрации с учетом (9)–(11), имеет вид

$$p(t)dt \propto I(t)dt = \Gamma^{(1)}(t)dt = \left|\sqrt{\omega_0}f_0\exp\left[-i\omega_0(t-t_0) + \frac{ik_0L}{c}\right] + \right.$$
$$\left. + \sqrt{\omega_1}f_1\exp\left[-i\omega_1(t-t_0) + \frac{ik_1L}{c}\right]\right|^2\frac{dt}{2V}, \tag{12}$$

где $k_{0,1}$ — волновые векторы, соответствующие частотам $\omega_{0,1}$, $L$ — длина канала связи (предполагается, что измерение проводится в точке на расстоянии $L$ от передающего конца).

Измерения амплитуды спектральных компонент $f_{0,1}$ реализуются при помощи пары узкополосных фильтров, вырезающих перед фотодетектированием частоты $\omega_{0,1}$, и того




Качественная схема криптосистемы. Сигнал от однофотонного источника направляется на «призму», за которой стоит экран, пропускающий сигнал с частотой либо $\omega_0$ (логический нуль, открыта верхняя диафрагма), либо $\omega_1$ (логическая единица, открыта нижняя диафрагма), либо обе частоты (контрольный сигнал, открыты обе диафрагмы). На приемном конце процедура измерения устроена аналогично. Открыта верхняя диафрагма — измерение $E_0$, открыта нижняя — измерение $E_1$, открыты обе — измерение $E(dt)$. Диафрагмы открыты либо закрыты в течение всей конкретной посылки

же самого фотодетектора. Вероятность регистрации, согласно (9)–(11), не зависит от времени:

$$p_c(t)dt \propto \Gamma^{(1)}(t)dt = \begin{cases} \dfrac{\hbar\omega_0}{V}|f_0|^2 dt, & \text{измерение } E_0, \\ \dfrac{\hbar\omega_1}{V}|f_1|^2 dt, & \text{измерение } E_1, \end{cases}$$

$$p_{0,1}(t)dt \propto \Gamma^{(1)}(t)dt = \begin{cases} \dfrac{\hbar\omega_0}{V}\cdot 1\cdot dt, & \text{измерение } E_0 \text{ для } \hat{\rho}_0, \\ 0 & \text{измерение } E_1 \text{ для } \hat{\rho}_0, \\ \dfrac{\hbar\omega_1}{V}\cdot 1\cdot dt, & \text{измерение } E_1 \text{ для } \hat{\rho}_1, \\ 0 & \text{измерение } E_0 \text{ для } \hat{\rho}_1. \end{cases} \tag{13}$$

Качественная схема криптосистемы представлена на рисунке. Перед входом в линию сигнал от однофотонного источника разлагается в спектр, из которого вырезаются либо одна из частот ($\omega_0$ или $\omega_1$), либо одновременно обе спектральные компоненты с частотами $\omega_0$ и $\omega_1$. Измерение $E(dt)$ реализуется при помощи быстрого фотодетектора, работающего в ждущем режиме. Именно в ждущем режиме факт наступления события (его регистрации) будет иметь место в случайный, не зависящий от воли экспериментатора момент времени. В этом состоит отличие от измерения $E(dt)$, которое осуществляется в заранее выбранный экспериментатором момент времени в интервале $(t, t+dt)$; вероятность регистрации в этот момент времени описывается плотностью $p_c(t)$. Нельзя при этом понимать измерение $E(dt)$ как измерение быстрым фотодетектором, перед которым в интервале $(t, t+dt)$ открывается входная диафрагма. Такая процедура тоже отвечает какому-то измерению, но не измерению $E(dt)$.

Интегральная вероятность регистрации к моменту времени $T$ дается выражением

$$P(T) = \int^{T} dt\, p_i(t), \quad i = c, 0, 1,$$

откуда дифференцированием по верхнему пределу может быть получена плотность вероятности в интервале времени $(t, t+dt)$.

Измерение $E(dt)$ по сути содержит информацию об «интерференции» различных спектральных компонент внутри одного квантового состояния (информацию об относительной фазе компонент с частотами $\omega_0$ и $\omega_1$). Поэтому принципиально важно, чтобы в разных посылках состояние $\hat{\rho}_c$ было приготовлено так, чтобы относительная фаза спектральных компонент была одинакова. В противном случае осциллирующая по времени («интерференционная») с частотой $\omega_1 - \omega_0$ составляющая в вероятности $p_c(t)$ в разных попытках не будет воспроизводиться в одни и те же моменты времени. Вопрос о приготовлении однофотонного состояния с фиксированной относительной фазой компонент может быть решен следующим образом. Пусть имеется двухуровневая система с невырожденным по спину электронным спектром (например, квантовая точка с кулоновским взаимодействием (см. детали в [29]). Резонансной подсветкой $\pi$-импульсом система может быть переведена в возбужденное (квазистационарное) состояние. Пусть длительность $\pi$-импульса существенно меньше времени излучательной рекомбинации ($\tau_\pi \ll \tau_R$). Длительность $\pi$-импульса может быть сделана существенно короче $\tau_R$, и при этом еще с запасом не нарушается условие резонансности подсветки [29]. Последнее означает, что момент возбуждения $t_0$ определен с точностью $\sim \tau_\pi \ll \tau_R$. После выключения $\pi$-импульса свободная эволюция системы «электрон в возбужденном состоянии + электромагнитное поле в вакуумном состоянии» приведет к рекомбинации электрона и появлению однофотонного пакета с характерной шириной спектра $\Delta\omega \approx 1/\tau_R$. Однофотонный пакет определяется как [30, 31]

$$|1_f\rangle = \sum_k f_k a^+_{\omega_k}|0\rangle, \quad \sum_k |f_k|^2 = 1. \tag{14}$$

Среднее число фотонов в пакете

$$n = \langle 1_f|a^+_{\omega_k} a_{\omega_k}|1_f\rangle = 1, \tag{15}$$

физически это означает, что регистрация идеальным широкополосным фототедектором (захватывающим все спектральные компоненты) приведет к одному срабатыванию с вероятностью единица. Регистрация же идеальным узкополосным детектором на частоте $\omega_n$ приведет к срабатыванию с вероятностью $|f_n|^2 < 1$.

Поскольку каждый раз система в момент времени $t_0$ стартует из одинакового состояния, то в разных посылках однофотонные пакеты одинаковы (фаза всех спектральных компонент, определяемая множителями $\exp(-i\omega_i t_0)$ одинакова в разных посылках). Вырезание из спектра двух узких спектральных компонент сохраняет их относительную фазу. Действительно, вырезание спектральных компонент формально описывается как действие проектора[1)]

$$E_0 + E_1 = (|1_{\omega_0}\rangle\langle 1_{\omega_0}| + |1_{\omega_1}\rangle\langle 1_{\omega_i}|),$$

после этого матрица плотности однофотонного волнового пакета переходит в новое состояние (см., например, [25, 26, 32])

---

[1)] Строго говоря, идеальный фильтр отвечает проектору на подпространство состояний с частотами $\omega_0$, $\omega_1$ и всеми числами заполнения, $E_{\omega_0} + E_{\omega_1} = \sum_{n=0}^{\infty}(|n_{\omega_0}\rangle\langle n_{\omega_0}| + |n_{\omega_1}\rangle\langle n_{\omega_1}|)$, однако это не меняет результатов.

$$\hat{\rho}_{in}(t) = \left\{\sum_k \exp\left[-i\omega_k(t-t_0)\right] f_k |1_{\omega_k}\rangle\right\} \times$$
$$\times \left\{\sum_{k'} \langle 1_{\omega'_k}| f^*_{k'} \exp\left[i\omega'_k(t-t_0)\right]\right\} \to \frac{1}{\mathrm{Tr}\{\hat{\rho}_{in}(t)(E_0+E_1)\}}(E_0+E_1) \times$$
$$\times \left\{\sum_k \exp\left[-i\omega_k(t-t_0)\right] f_k |1_{\omega_k}\rangle\right\} \left\{\sum_{k'} \langle 1_{\omega'_k}| f^*_{k'} \exp\left[i\omega'_k(t-t_0)\right]\right\} (E_0+E_1) \to$$
$$\to \frac{1}{|f_0|^2+|f_1|^2} \left\{\exp\left[-i\omega_0(t-t_0)\right] f_0 |1_{\omega_0}\rangle + \exp\left[-i\omega_1(t-t_0)\right] f_1 |1_{\omega_1}\rangle\right\} \times$$
$$\times \left\{\langle 1_{\omega_0}| f^*_0 \exp\left[i\omega_0(t-t_0)\right] + \langle 1_{\omega_1}| f^*_1 \exp\left[i\omega_1(t-t_0)\right]\right\}. \qquad (16)$$

Физически это означает, что если за фильтрами поставить идеальный широкополосный фотодетектор, то при большом числе повторяющихся испытаний он будет срабатывать лишь в доле $\mathrm{Tr}\{\hat{\rho}_{in}(t)(E_0+E_1)\}$ случаев от их полного числа.

Относительная фаза компонент с частотами $\omega_0$ и $\omega_1$ определяется их фазой в момент приготовления, что в принципе достижимо, как это описано выше. Таким образом, при условии $\tau_\pi \ll \tau_R \ll 1/|\omega_1-\omega_0|$ можно считать, что в различных посылках интерференционная картина по времени стоит на месте. В различных посылках интерференционная картина «плывет» лишь в меру неточности начального момента приготовления $\delta t_0$ на величину $\delta t_0 \le \tau_\pi \ll T = 2\pi/|\omega_1-\omega_0|$, что существенно меньше периода временно́й интерференционной картины.

При длительности $\pi$-импульса $\tau_\pi \sim 10^{-12}$ с (см. [29]) и времени излучательной рекомбинации $\tau_R \sim 10^{-10}$ с (при этом ширина спектра исходного однофотонного состояния $\Delta\omega \sim 10^{10}$ Гц), вырезании спектральных компонент шириной $\sigma \approx 10^7$ Гц и расстоянии между ними $\delta\omega = |\omega_1-\omega_0| \sim 10^8$ Гц (что еще очень далеко от достижимых на сегодняшний день рекордов) требуемое быстродействие фотодетектора удовлетворяется при $\tau_{det} \sim 10^{-9}$ с.

При этом цепочка неравенств $\tau_\pi \ll \tau_R \ll \tau_{det} \ll 1/\delta\omega$ удовлетворяется с запасом. Разумеется, что эффективность за счет вырезания узких спектральных компонент шириной $\sigma \sim 10^7$ Гц из спектра шириной $\Delta\omega \sim 10^{10}$ Гц составляет $\sim \sigma/\Delta\omega \sim 10^{-3}$. Но по-крайней мере вопрос о строго однофотонном источнике решается в принципе.

Оценим точность в фиксации длины канала связи. Изменения длины оптоволоконной линии также приводят к размытию интерференционной картины из-за наличия в формуле (12) в показателе экспоненты слагаемых с $k_{0,1}L$. Изменения относительной фазы спектральных компонент за счет вариации длины линии $\delta L$ должны удовлетворять условию

$$|k_1-k_0|\delta L \approx |\omega_1-\omega_0|\delta L/c \ll 2\pi,$$

допустимые вариации длины линии должны приводить к относительному сдвигу фазы, много меньшему, чем $2\pi$. Это дает оценку

$$\delta L \ll 2\pi c/\delta\omega \approx 10^2 \text{ см},$$

что является достаточно мягким условием.

Интерференционная картина также может размываться, за счет того что вектор поляризации в различных частотных компонентах вращается с разной скоростью. Однако

если положение кабеля фиксировано, то интерференционная картина может быть заранее «откалибрована». В этом случае ее изменение будет связано только с разными оптическими путями частотных компонент, т. е. вариацией длины линии. Последнее условие, по-видимому, является некритичным. Частотная дисперсия диэлектрической постоянной оптоволокна также может приводить к сглаживанию амплитуды осцилляций интерференционной картины. Чем длиннее линия, тем сильнее сглаживание. Однако, как показывают оценки работы [21], при ширине спектральных компонент $\sigma \approx 10^7$ Гц, дисперсия сказывается при гораздо большей длине, чем затухание. Затухание не влияет на секретность системы, а лишь уменьшает ее эффективность за счет увеличения доли холостных измерений.

Рассмотренные выше состояния с бесконечно узкими спектральными компонентами являются идеализацией и непригодны для передачи по каналу связи из-за формально бесконечной протяженности по времени. В реальных экспериментах можно приготовить состояния лишь с конечной шириной линии (приготовление строго монохроматических фотонных состояний потребовало бы формально бесконечного времени). В качестве информационных состояний можно использовать однофотонные состояния вида (14) с гауссовскими спектральными плотностями

$$|1_{\omega_{0,1},c}\rangle = \int_0^\infty f_{0,1,c}(\omega)a^+(\omega)|0\rangle, \quad [a(\omega), a^+(\omega')] = \delta(\omega - \omega')\hat{I}, \tag{17}$$

$$E^{(+)}(x,t) = \frac{1}{\sqrt{2\pi}} \int_0^\infty \exp\left[-i\omega\left(t - \frac{x}{c}\right)\right] a(\omega)d\omega, \tag{18}$$

$$f_{0,1}(\omega) = \frac{1}{(2\pi\sigma^2)^{1/4}} \exp\left[-\frac{(\omega - \omega_{0,1})^2}{4\sigma^2}\right] \exp(-i\omega t_0) \tag{19}$$

и контрольного состояния, содержащего обе узкополосные гауссовские компоненты с амплитудами $f_0$ и $f_1$:

$$f_c(\omega) = \frac{\text{const}}{(2\pi\sigma^2)^{1/4}} \left\{ f_0 \exp\left[-\frac{(\omega - \omega_0)^2}{4\sigma^2}\right] + f_1 \exp\left[-\frac{(\omega - \omega_1)^2}{4\sigma^2}\right] \right\} \exp(-i\omega t_0), \tag{20}$$

где нормировочная константа

$$\text{const} = \left\{ |f_0|^2 + |f_1|^2 + \sqrt{2}\text{Re}\left[f_0 f_1^*\right] \exp\left[-\frac{(\omega_0^2 + \omega_1^2 - \omega_0\omega_1)}{2\sigma^2}\right] \right\}^{-1}. \tag{21}$$

Измерения узких спектральных компонент при помощи соответствующих гауссовских фильтров приводят к слабой зависимости исходов измерений от времени, в отличие от предыдущего рассмотрения случая строго монохроматических состояний, где вероятность исхода от времени не зависела. Соответствующая плотность вероятности результатов имеет вид

$$p(t)dt \propto I(t)dt = 2\sqrt{2\pi\sigma^2} \exp\left[-2\sigma^2(t - t_0 - L/c)^2\right] dt, \tag{22}$$

откуда, в частности, следует, что вероятность регистрации фотодетектором в ждущем режиме стремится к единице, лишь если время $T$ ожидания превышает обратную ширину

спектра ($T \geq 1/\sigma$). Данное обстоятельство совпадает с интуитивными представлениями о длительном времени регистрации узкополосного состояния.

Плотность вероятности исходов измерений для контрольного состояния имеет вид

$$p_c(t)dt \propto I(t)dt = \text{const} \cdot 2\sqrt{2\pi\sigma^2}\exp\left[-2\sigma^2(t-t_0-L/c)^2\right] \times \\ \times \left\{|f_0|^2 + |f_1|^2 + 2\mathrm{Re}\left(f_0 f_1^* \exp\left[-i(\omega_0-\omega_1)(t-t_0-L/c)\right]\right)\right\} dt. \qquad (23)$$

Интерференционная осциллирующая составляющая является хорошо выраженной при условии $\sigma \ll |\omega_1 - \omega_0|$.

## 4. ЗАКЛЮЧЕНИЕ

Несмотря на различные варианты предложенных квантовых криптосистем, по мнению автора, существует некоторая неопределенность, связанная со следующим. Доказательство секретности квантовой криптографии на двух неортогональных состояниях, предложенное в [3], подразумевает стационарность состояний и их принадлежность одной энергии. В противном случае для нестационарных состояний проекторы $\overline{E}_0$ и $\overline{E}_1$ были бы разными в разные моменты времени. Неортогональность стационарных состояний подразумевает, что они отвечают одной энергии. В противном случае стационарные состояния, принадлежащие разным энергиям, были бы автоматически ортогональны. В этом смысле протокол на стационарных состояниях существует как бы вне времени. Попытки ввести в протокол обмена время явно [14, 17] все равно при доказательстве секретности используют рассуждения работы [3] для стационарных состояний (см., например, [17]). Стационарные же состояния являются бесконечно протяженными во времени. Аналогичная ситуация имеет место и в данной работе. Доказательство секретности для состояний с бесконечно узкими, а значит, и бесконечно протяженными во времени спектральными плотностями также апеллирует к рассуждениям работы [3]. Для случая, когда пространство состояний системы является бесконечномерным (описывается непрерывной переменной), доказательство секретности той же степени строгости, что и [3], насколько известно, отсутствует. В этом смысле, на наш взгляд, отсутствует доказательство секретности квантовых криптосистем, работающих в режиме реального времени.

В заключение выражаю благодарность Б. А. Волкову, С. С. Назину, С. Т. Павлову и И. И. Тартаковскому за плодотворные обсуждения. Работа поддержана Российским фондом фундаментальных исследований (проект 96-02-19396).

## Литература

1. S. Wiesner, *Conjugate Coding*, Sigact News. **15**, 78 (1983); исходный текст датирован 1970 г.
2. C. H. Bennett and G. Brassard, in *Proceedings of IEEE Intern. Conf. on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, p. 175.
3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
4. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

5. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
6. A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).
7. A. Muller, J. Brequet, and N. Gisin, Europhys. Lett. **30**, 809 (1994).
8. R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Contemp. Phys. **36**, 149 (1995).
9. S. J. D. Phoenix and P. D. Townsend, Contemp. Phys. **36**, 165 (1995).
10. C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
11. J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).
12. J. D. Franson and H. Ilves, J. Mod. Opt. **41**, 2391 (1994).
13. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, in *Advances in Cryptography–Proceedings of Crypto'96*, August 1996, Springer-Verlag, Berlin (1996).
14. L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
15. M. Koashi and N. Imoto, Phys. Rev. Lett. **77**, 2137 (1996).
16. E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
17. M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
18. A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995).
19. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793, (1997).
20. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ **62**, 256 (1996).
21. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ **63**, 646 (1996); **64**, 813 (1996); С. Н. Молотков, Письма в ЖЭТФ **64**, 652 (1996); **65**, 559 (1997); **66**, 736 (1997).
22. С. Н. Молотков, С. С. Назин, Письма в ЖЭТФ **66**, 742 (1997).
23. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
24. А. С. Холево, *Вероятностные и статистические аспекты квантовой теории*, Наука, Москва (1980).
25. И. фон Нейман, *Математические основы квантовой механики*, Наука, Москва (1964).
26. P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics*, Springer Lecture Notes in Physics, Vol. 31 (1995).
27. A. N. Kolmogorov, Giornale dell'Istituto degli Attuari **4**, 83 (1933); см. также П. Л. Хенкенен, А. Тортра, *Теория вероятностей и некоторые ее приложения*, Наука, Москва (1974).
28. Я. Перина, *Когерентность света*, Мир, Москва (1974).
29. Ф. В. Крашенинников, Л. А. Опенов, С. Н. Молотков, С. С. Назин, ЖЭТФ **112**, 1257 (1997).
30. R. J. Glauber, Phys. Rev. **130**, 2529 (1963).
31. R. A. Campos, B. E. Salech, and M. Teich, Phys. Rev. A **42**, 4127 (1990).
32. К. Хелстром, *Квантовая теория проверки гипотез и оценивания*, Мир, Москва (1979).