Письма в ЖЭТФ, том 63, вып.11, стр.882 - 887 © 1996г. 10 июня

КВАНТОВАЯ КРИПТОГРАФИЯ НА СООТНОШЕНИИ НЕОПРЕДЕЛЕННОСТЕЙ ЭНЕРГИЯ–ВРЕМЯ

С.Н.Молотков, С.С.Назин

Институт физики твердого тела РАН

142432 Черноголовка, Московская обл., Россия

Поступила в редакцию 23 апреля 1996 г.

Предлагается новая квантовая криптосистема, основанная на фундаментальном соотношении неопределенностей энергия – время. Такая криптосистема может быть реализована как с использованием бифотонных состояний, так и на одиночных фотонах.

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

В основе квантовой криптографии лежат следующие два обстоятельства. Во-первых, стохастическая природа результатов процесса измерения в квантовой механике приводит к тому, что использование некоторых специальным образом приготовленных состояний дает возможность двум пространственно удаленным пользователям, проводящим серию измерений подходящей физической величины, получить две полностью коррелированные случайные последовательности нулей и единиц, которые могут быть использованы в качестве ключа [1–9]. Во-вторых, невозможность в общем случае восстановить волновую функцию системы, которой она описывалась до измерения, по результатам этого измерения [10] позволяет обнаружить подслушивателя или лицо, пытающееся вмешаться в процесс генерации ключа.

В данной работе предлагается новая криптосистема, в которой защита от вмешательства третьего лица основана на квантово-механическом соотношении неопределенностей энергия – время.

Рассматриваемая криптосистема основана на совместном измерении состояний бифотонного поля двумя пользователями, хотя, как будет видно из дальнейшего, *такая криптосистема может быть построена с использованием одиночных фотонных состояний с разными частотами, что очень важно с точки зрения практической реализации.*

Бифотонное поле имеет вид

$$|\Psi\rangle = \exp(-i\omega_0 t)\int g(\omega)|1\rangle_\omega |1\rangle_{\omega_0-\omega} d\omega, \qquad (1)$$

где $|1\rangle_\omega$ – состояние одной фотонной моды с частотой ω, ω_0 – некоторая фиксированная частота (имеющая смысл суммы частот двух фотонов, входящих в бифотон), $g(\omega)$ – функция, определяющая ширину спектра бифотонов. Такое поле может быть получено в процессе параметрического рассеяния (распад возбуждающего фотона с энергией $\hbar\omega_0$ за счет оптической нелинейности $\chi^{(2)}$ на пару фотонов в "запутанном" состоянии (1)) [11–13] или в результате некаскадных двухфотонных переходов в атомах, приготовленных в подходящем возбужденном состоянии.

Генерация ключа основана на использовании фотодетекторов с различной полосой регистрации. Предположим, что два пользователя, A и B, регистрируют фотоны с помощью фотодетекторов, имеющих центральные частоты $\omega_{A,B}$

и ширины полос регистрации $\gamma_{A,B}$. Пусть атом приготовлен в возбужденном состоянии в момент времени $t = 0$, а фотоны были зарегистрированы пользователями в моменты времени t_A^0 и t_B^0, соответственно. Функция корреляции интенсивностей бифотонного поля при совместном измерении двумя пользователями зависит от относительной задержки приведенных времен регистрации $T = t_B - t_A$, где $t_{A,B} = t_{A,B}^0 - r_{A,B}/c$ ($r_{A,B}$ – расстояния пользователей от источника, c – скорость света в среде) [11, 13] и имеет вид

$$P(T) = (2\pi\gamma_A\gamma_B)^2 \frac{\theta(T)\exp(-2\gamma_B T) + \theta(-T)\exp(2\gamma_A T)}{\Omega^2 + (\gamma_A + \gamma_B)^2}, \qquad (2)$$

$$\Omega = \omega_0 - \omega_A - \omega_B.$$

Здесь $\theta(T)$ – ступенчатая функция.

В случае регистрации бифотонного поля двумя узкополосными детекторами ($\gamma_{A,B} \to 0$) срабатывание последних имеет место лишь при $\omega_A + \omega_B = \omega_0$, то есть когда пользователи применяют детекторы с дополнительными частотами, и

$$P(T) \propto \delta(\omega_0 - \omega_A - \omega_B) \equiv \text{корреляция фотонов по энергии.} \qquad (3)$$

При детектировании поля излучения (1) двумя широкополосными фотодетекторами ($\gamma_{A,B} \to \infty$) из (2) следует, что

$$P(T) \propto \delta(t_B - t_A) \equiv \text{корреляция по времени регистрирования фотонов.} \qquad (4)$$

При регистрации узкополосными фотодетекторами ($\gamma \to 0$, уравнение (3)) разность времен регистрации фотонов пользователями T может принимать любые значения в интервале $-\infty < T < \infty$.

В случае регистрации широкополосными детекторами ($\gamma \to \infty$, уравнение (4)) разность приведенных моментов регистрации фотонов с большой точностью ($\sim 1/\gamma \to 0$) равна нулю, однако при этом ничего нельзя сказать об энергии (частоте) регистрируемых фотонов.

Протокол генерации ключа выглядит следующим образом:

1) выбираются две фиксированные частоты ω_1 и ω_2, такие, что $\omega_1 + \omega_2 = \omega_0$. В каждом измерении пользователи A и B независимо друг от друга случайным образом выбирают либо один из узкополосных фотодетекторов с центральными частотами ω_1 или ω_2, либо широкополосный;

2) после проведения серии измерений отбрасываются те измерения, где не было срабатывания хотя бы одного из фотодетекторов;

3) через открытый канал открываются измерения, в которых были использованы однотипные фотодетекторы (широкополосный или узкополосные, но не сообщается, какой из узкополосных – ω_1 или ω_2);

4) поскольку рассматриваются только те измерения, где было срабатывание обоих фотодетекторов, измерения, где обоими пользователями применялись узкополосные фотодетекторы, дают полную корреляцию измерений, которые и составляют ключ. Например, если A использовал детектор с ω_1, то срабатывание у B имеет место, если он проводил измерение детектором с ω_2 (измерениям в этой ситуации соответствует логическая 1), и наоборот, если A использовал детектор, настроенный на ω_2, то B измерял ω_1 (логический 0).

Для обнаружения возможного подслушивания на этапе генерации ключа используются те измерения, в которых обоими пользователями были выбраны

широкополосные фотодетекторы. В этом случае A и B фиксируют относительную задержку времени регистрации $t_B - t_A$ (считается, что длина линии известна). Если подслушивания не было, то $T = t_B - t_A = 0$ (с точностью до $1/\gamma_{A,B} \to 0$); наличие же подслушивателя в линии приведет к $T \neq 0$. Действительно, чтобы получить информацию о ключе (фотон с какой частотой, ω_1 или ω_2, присутствует в линии), подслушиватель вынужден применять узкополосный фотодетектор с шириной полосы регистрации $\gamma_* \to 0$, поскольку широкополосный фотодетектор не позволяет различать фотоны с энергиями ω_1 и ω_2, в которых и содержится информация о ключе. Поскольку типы фотодетекторов пользователи A и B выбирают случайно, то будут ситуации, когда A и B использовали широкополосные фотодетекторы (то есть должны были бы получить $T = 0$), а подслушиватель использовал узкополосный детектор, то есть измерил энергию фотона с точностью $\gamma_* \to 0$. Но согласно квантово-механическому соотношению неопределенностей энергия–время

$$\Delta E \Delta t \geq \hbar, \tag{5}$$

такое измерение не может быть осуществлено за время, меньшее чем $\hbar/\gamma_*$. Следовательно, пользователи A и B смогут обнаружить вторжение третьего лица по систематическому отклонению разности приведенных времен регистрации фотонов $T = t_B - t_A$ от нуля.

Следует отметить, что ситуация с соотношением (5) не столь проста, как с соотношениями неопределенности для других переменных, таких как координата – импульс или различные компоненты спина. Несмотря на очень длинную историю [13–20], вопрос о справедливости соотношения (5) и интерпретации входящих в него величин ΔE и Δt дискутируется по сей день (см. обзор [20]). Согласно [20], вопрос о справедливости соотношения (5) сводится к справедливости одного из следующих утверждений:

1) разброс значений энергии квантовомеханической системы ΔE до и после измерения удовлетворяет неравенству (5), где Δt представляет собой длительность процесса измерения, то есть сколь угодно быстрые измерения, не изменяющие состояния квантовой системы, *невозможны*;

2) возможны *сколь угодно быстрые* измерения, невозмущающие энергию квантовой системы (нарушающие неравенство (5)).

Вообще говоря, имеются примеры гамильтонианов, явно зависящих от времени (см., например, [14, 15]), нарушающих неравенство (5). Таким образом, вопрос о справедливости (5) сводится к возможности или невозможности реализации тех или иных гамильтонианов, допускаемых квантовой механикой как формальной математической схемой [20]; при этом существенным моментом является то обстоятельство, что физические реализации гамильтонианов, приводящих к нарушению соотношения (5), до сих пор неизвестны. В то же время очевидно, что имеет смысл рассматривать лишь физически реализуемые гамильтонианы [16–19]. Следовательно, в настоящий момент есть все основания рассматривать соотношение (5) как фундаментальный закон природы. Мы будем придерживаться именно этой ортодоксальной точки зрения [16–19], считая, что *точное измерение энергии фотона за сколь угодно малое время невозможно.*

В качестве иллюстрации рассмотрим ситуацию, когда пользователь A проводит измерение широкополосным фотодетектором ($\gamma_A \to \infty$), а второй (подслушиватель, который в данном примере играет роль пользователя B) –

узкополосным ($\gamma_B \to 0$). Для этого случая функция $P(T)$ изображена на рис.1, из которого видно, что пользователь B всегда регистрирует фотон с некоторой задержкой относительно A, причем с равной вероятностью можно получить любую задержку. Для того чтобы качественно понять этот результат, процесс фотодетектирования можно представлять себе следующим образом. Будем считать, что фотодетектор состоит из поглотителя (двухуровневого "атома"), туннельно связанного с макроскопическим "электродом" (рис.2a, b). Время жизни электрона на квазистационарном уровне после поглощения фотона определяется его шириной (это время, по существу, является временем измерения: в среднем за это время электрон переходит из квантовой системы в классическую – "электрод"). В случае широкополосного фотодетектора ($\gamma_A \to \infty$) ширина уровня велика; при этом невозможно точно определить частоту поглощаемого фотона, зато процесс детектирования является быстрым из-за быстрого ухода в "электрод". В случае узкополосного фотодетектора ($\gamma_B \to 0$) поглощение имеет место только при совпадении частоты фотона с расстоянием между уровнями. Сам же процесс измерения, уход электрона в "электрод", происходит медленно, в пределе $\gamma_B = 0$ электрон "болтается" между уровнями [21] и не уходит в "электрод", так что процесс измерения (детектирования) формально длится бесконечно долго (что и приводит к задержке регистрации фотона пользователем B).

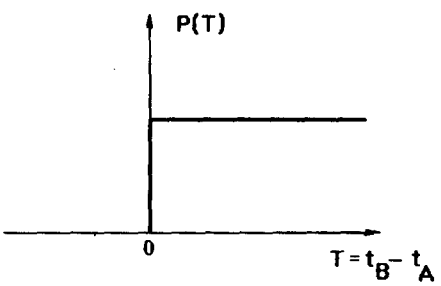

Рис.1. Функция корреляции интенсивностей $P(T)$ для случая измерения при помощи фотодетекторов с $\gamma_A \to \infty$ и $\gamma_B \to 0$

Таким образом, если справедливо соотношение (5) (утверждение 1)), то невозможно точно измерить частоту узкополосным фотодетектором за сколь угодно малое время (иначе бы нарушалось неравенство (5)), и этим обстоятельством можно воспользоваться для обнаружения подслушивания.

Заметим, что подслушиватель не может быть обнаружен, если A и B используют лишь узкополосные фотодетекторы. Действительно, в этом случае подслушиватель может с помощью узкополосных детекторов (например, поставив их в ряд в порядке возрастания частоты) определить, фотон с какой частотой имеется в линии (по тому, какой из его фотодетекторов сработает). Затем он своим источником перепосылает к B фотон с той частотой, которую он измерил. Очевидно, что в такой ситуации обнаружить подслушивателя в линии нельзя.

Подчеркнем, что *неизбежное появление задержки при измерениях пользователей A и B в описанном протоколе связано не с ухищрениями пользователей, а гарантируется фундаментальным соотношением (5).* Увеличи-

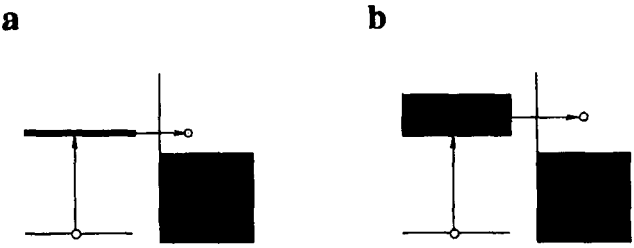

Рис.2. *а*) Процесс измерения узкополосным фотодетектором ($\gamma \to 0$); *б*) процесс измерения широкополосным фотодетектором ($\gamma \to \infty$). В правых частях изображена макроскопическая часть фотодетектора – "электрод"

вая долю измерений, в которых используются широкополосные фотодетекторы, можно сделать вероятность обнаружения подслушивателя в линии сколь угодно близкой к единице.

Ясно, что для подслушивателя ситуация тем хуже, чем меньше разница между ω_1 и ω_2 (на сегодняшний день, по-видимому, легко достижима разность $|\omega_1 - \omega_2| \sim 10^5\,\text{с}^{-1}$ на частоте $\omega_1 \approx \omega_2 \sim 10^{15}\,\text{с}^{-1}$ (при длине волны $\lambda_0 = 1.3$ мкм, соответствующей окну прозрачности оптоволокна, $\omega \sim 10^{15}\,\text{с}^{-1}$). Для того чтобы отличать фотоны с частотами ω_1 и ω_2, подслушиватель должен измерять частоту фотонов с точностью не хуже чем $10^5\,\text{с}^{-1}$, что приведет к задержке порядка 10^{-5} с при подслушивании (то есть эффективному удлиннению линии на 3 км). В то же время, разность приведенных моментов регистрации фотонов T при отсутствии подслушивания может быть сделана достаточно малой даже при не очень широкополосных фотодетекторах. При ширине полосы фотодетектора $\gamma \sim 10^9\,\text{с}^{-1}$ (то есть порядка естественной ширины атомного уровня) $T \sim 1/\gamma \sim 10^{-9}$ с (то есть в контексте данной проблемы фотодетектор с шириной полосы пропускания $\sim 10^9\,\text{с}^{-1}$ может уже рассматриваться как широкополосный).

Сделаем в заключение одно важное замечание. Аналогичную схему можно построить, не используя бифотонные состояния, если пользователь A имеет возможность посылать одиночные фотоны с близкими энергиями $\hbar\omega_1$ и $\hbar\omega_2$, моменты испускания которых известны с достаточно высокой точностью. Для этого, например, можно воспользоваться квантовыми точками, в которых время жизни электрона на возбужденном размерно-квантованном уровне по порядку величины составляет 10^{-9} с; если электрон забрасывается на такой уровень коротким (пикосекундным) импульсом, можно считать, что момент его вылета в линию известен с точностью до 10^{-9} с. Поэтому, если имеются два такого рода узкополосных источника фотонов с частотами, отличающимися на величину порядка $10^5\,\text{с}^{-1}$, они могут быть использованы для построения криптосистемы на соотношении неопределенностей энергия – время. Подобная схема имеет преимущества по сравнению с интерференционными схемами, поскольку она не требует периодической юстировки интерферометра с длинной базой [7]. Данная криптосистема позволяет также распространять ключ по сети равноправных пользователей (путем передачи по цепочке) на расстояния,

превышающие длину затухания в оптоволокне, аналогично тому, как это описано в [22].

Мы благодарны С.В.Иорданскому, М.В.Лебедеву, С.Т.Павлову и И.И.Тартаковскому 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.H.Bennet, Phys. Rev. Lett. **68**, 3132 (1992).
3. C.H.Bennet, G.Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
4. A.K.Ekert, J.G.Rarity, P.R.Tapster, and G.M.Palma, Phys. Rev. Lett. **69**, 1293 (1992).
5. R.J.Hughes, D.M.Alde, P.Dyer et al., Contemporary Phys. **36**, 149 (1995).
6. S.J.D.Phoenix and P.D.Townsend, Contemporary Phys. **36**, 165 (1995).
7. C.Marand and P.D.Townsend, Optics Lett. **20**, 1695 (1995).
8. S.J.D.Phoenix, Phys. Rev. **A48**, 96 (1993).
9. S.M.Barnett and S.J.D.Phoenix, Phys. Rev. **A48**, R5 (1993).
10. W.K.Wootters and W.H.Zurek, Nature. **299**, 802 (1982).
11. Д.Н.Клышко, *Фотоны и нелинейная оптика*, М.: Наука, 1980.
12. D.N.Klyshko, Phys. Lett. **A128**, 133 (1988).
13. Д.Н.Клышко, УФН **158**, 327 (1989).
14. Y.Aharonov and D.Bohm, Phys. Rev. **122**, 1649 (1961).
15. Y.Aharonov and J.L.Safko, Ann. Phys. **91**, 279 (1975).
16. L.D.Landau and R.Peierls, Ztschr. für Phys. **69**, 56 (1931).
17. Л.И.Мандельштам, И.Е.Тамм, Известия АН СССР, сер. физ. **9**(1/2), 122 (1945).
18. Н.С.Крылов, В.А.Фок, ЖЭТФ **17**, 93 (1947).
19. В.А.Фок, ЖЭТФ **42**, 1135 (1962).
20. В.В.Додонов, В.И.Манько, Труды ФИАН **183**, 52 (1987).
21. S.Flügge, *Practical Quantum Mechanics II*, ch.V, 180, Springer-Verlag, Berlin - Heidelberg - New York, 1971.
22. С.Н.Молотков, С.С.Назин, Письма в ЖЭТФ **63**, 646 (1996).