Письма в ЖЭТФ, том 65, вып.7, стр.559 - 564 © 1997г. 10 апреля

О СТРАТЕГИЯХ ГРУБОГО И ПРОЗРАЧНОГО ПОДСЛУШИВАНИЯ В КВАНТОВОЙ КРИПТОСИСТЕМЕ

С.Н.Молотков

Институт физики твердого тела РАН

142432 Черноголовка Московской обл., Россия

Поступила в редакцию 3 марта 1997 г.

Обсуждается конфиденциальность квантовой криптосистемы, основанной на соотношении неопределенностей энергия–время, по отношению к стратегиям грубого и прозрачного подслушивания.

PACS: 03.65.-w, 89.70.+c

В квантовой криптографии носителями информации являются квантовые состояния. Доказано, что невозможно скопировать заранее неизвестное состояние [1]. Секретность квантовых криптосистем основывается на том, что любое измерение над набором неортогональных состояний, позволяющее извлекать ненулевую информацию, приводит к их изменению [1, 2].

Условно стратегии подслушивания можно разделить на два типа [3]. Грубое подслушивание сводится к измерению над носителем информации. При прозрачном подслушивании информация извлекается из вспомогательного состояния (ancilla), которое приготавливается и "подцепляется" подслушивателем к носителю. После этого измерение проводится над состоянием ancilla.

Различные стратегии применительно к квантовой криптосистеме на двух неортогональных состояниях обсуждалась недавно в работах [4–6].

В этой работе мы хотим предложить физическую реализацию стратегии прозрачного подслушивания в криптосистеме [7], основанную на неразрушающем измерении частотного спектра сигнала.

Для описания состояния однофотонного волнового пакета удобно воспользоваться представлением в [8–10]. Оператор однофотонного волнового пакета имеет вид

$$\hat{A}^+(f) = \int_0^\infty f(\omega)\hat{a}^+(\omega)d\omega, \tag{1}$$

где $f(\omega)$ – комплексная амплитуда, $\hat{a}^+(\omega)$ – оператор рождения фотона в монохроматическом фоковском состоянии, удовлетворяющий бозевским коммутационным соотношениям. Операторы $\hat{A}(f)$ и $\hat{A}^+(f)$ также удовлетворяют бозевским коммутационным соотношениям при условии, что амплитуда $f(\omega)$ нормирована на единицу

$$\int_0^\infty |f(\omega)|^2 d\omega = 1. \tag{2}$$

Поле, отвечающее однофотонному волновому пакету, получается действием оператора рождения (1) на вакуумное состояние:

$$|1\rangle_f = \hat{A}^+(f)|0\rangle = \int_0^\infty f(\omega)\hat{a}^+(\omega)|0\rangle d\omega = \int_0^\infty f(\omega)|1_\omega\rangle d\omega, \tag{3}$$

где $|1_\omega\rangle$ – монохроматическое однофотонное состояние.

Протокол генерации ключа в схеме [7] состоит в посылке одним из законных пользователей A к другому – B случайным образом одного из трех однофотонных волновых пакетов. Два из них узкополосные с несущими частотами ω_1 и ω_2 (логический 0 и логическая 1) и шириной спектра $\sigma_{1,2}$ (далее считаем, что $\sigma_1 = \sigma_2 = \sigma$) не перекрываются (ортогональны). Третий однофотонный волновой пакет с короткой по времени длительностью и соответственно широким частотным спектром необходим для обнаружения попыток подслушивания. Секретность схемы на неортогональных состояниях гарантируется теоремой о запрете клонирования таких состояний [1,2]. Для ортогональных состояний подобная теорема отсутствует, поэтому конфиденциальность гарантируется соотношением неопределенностей энергия–время [7]. Точнее говоря, тем обстоятельством, что однофотонный волновой пакет со спектральной шириной σ для систематической регистрации требует времени не меньше, чем $1/\sigma$ (обсуждение различных точек зрения см., например, в [11–15]).

Третий сигнал имеет ширину спектра $\sigma_\infty \gg |\omega_1 - \omega_2|$ и несущую частоту $\omega_\infty \approx \omega_{1,2}$, соответствующая длительность этого сигнала – $\Delta t \approx 1/\sigma_\infty \ll 1/|\omega_1 - \omega_2|$.

Пользователь B в каждом измерении случайно и независимо от A выбирает один из двух узкополосных фотодетекторов, настроенных на частоту ω_1 или ω_2, или широкополосный фотодетектор. После проведения серии измерений пользователь B через открытый канал сообщает, какой тип фотодетекторов использовался в каждом отдельном измерении – узкополосный или широкополосный, но в случае узкополосных не сообщает, какой именно. Измерения, в которых применялись узкополосные фотодетекторы, дают идентичную последовательность 0 и 1 – ключ. Для детектирования возможных попыток подслушивания используются измерения, в которых A посылал B короткие по времени сигналы. Время вылета таких сигналов у A, а также время прилета к B, известны с точностью Δt.

Подслушиватель, чтобы иметь информацию о ключе, должен отличать 0 от 1 (ω_1 от ω_2). Для этого необходимо проводить измерения узкополосными фотодетекторами с полосой пропускания не хуже σ, но такие измерения, согласно соотношению неопределенностей, не могут быть сделаны систематически за времена меньшие, чем $\Delta T \geq 1/\sigma \gg \Delta t$. Из-за случайного выбора типа сигнала пользователем A подслушиватель неизбежно попадет на ситуации, когда он проводил измерения узкополосным фотодетектором, а в линию был послан сигнал с широким спектром. При этом разность между временами вылета и прилета такого пакета известна с точностью $\Delta t \ll \Delta T$, гораздо лучшей, чем задержка ΔT, вносимая подслушивателем при измерении.

Для получения количественных оценок потребуется конкретная форма сигналов. Будем считать для определенности, что спектральная форма всех трех сигналов является гауссовой:

$$f_{1,2,\infty}(\omega) = \frac{1}{(2\pi\sigma_{1,2,\infty}^2)^{1/4}} \exp\left(-\frac{(\omega - \omega_{1,2,\infty})^2}{2\sigma_{1,2,\infty}^2}\right). \tag{4}$$

Интенсивность однофотонного волнового пакета может быть представлена в виде

$$I_{1,2,\infty}(t) = 2\frac{\sigma_{1,2,\infty}}{\sqrt{\pi}} \exp\left(-\sigma_{1,2,\infty}^2 t^2\right). \tag{5}$$

Вероятность регистрации фотона во временном окне ΔT равна

$$P(\Delta T) = \int_0^{\Delta T} I(t)dt = \Phi(\sigma_{1,2,\infty}\Delta T), \quad \Phi(x) = \frac{2}{\sqrt{\pi}}\int_0^x \exp(-t^2/2), \qquad (6)$$

где $\Phi(x)$ – интеграл ошибок.

Формула (6) представляет собой оценку времени наступления события (регистрации), которая следует из соотношений Мандельштама–Тамма [12]. Для подобного типа экспериментов, когда регистрирующее устройство работает в режиме ожидания и эксперимент прекращается, когда ожидаемое событие произошло, оценка (6), конечно, является справедливой (см. обсуждение в [15]).

Если детектируется широкополосный сигнал, то вероятность прохождения однофотонного волнового пакета в регистрирующее устройство во временное окно ΔT описывается функцией $\Phi(\sigma_\infty \Delta T)$, которая быстро стремится к единице, если $\Delta T \geq 3\sigma_\infty$. Последнее означает, что задержки по времени ΔT для короткого сигнала, которые превышают $3\sigma_\infty$, детектируются с вероятностью, близкой к единице. Разброс времен измерений узкополосных сигналов не может быть меньше времени ожидания осуществления события. Последний не меньше, чем обратная ширина спектра сигнала $\approx 1/\sigma$ (время, требуемое на "прохождение" в регистрирующее устройство однофотонного волнового пакета). Измерение подслушивателем узкополосным фотодетектором с шириной полосы σ широкополосного сигнала сводится к вырезанию, например, фильтром из широкого спектра линии порядка σ с последующей регистрацией. Вероятность детектирования узкой полосы из широкого спектра за время ΔT не превосходит $P(\Delta T) \leq |f_\infty|^2 \Phi(\sigma \Delta T) \leq (\sigma/\sigma_\infty)\Phi(\sigma\Delta T)$ (здесь $f_\infty \approx 1/\sqrt{\sigma_\infty}$ – амплитуда широкополосного сигнала в максимуме).

Качественно измерительная схема для грубого подслушивания представлена на рис.1.

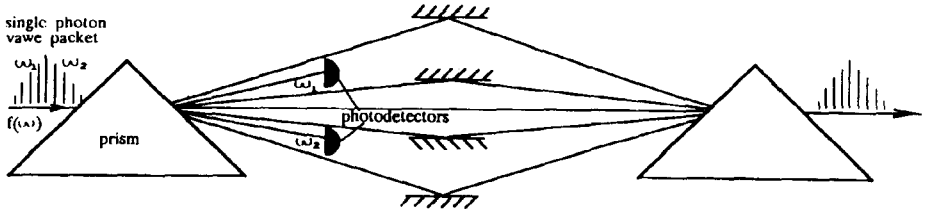

Рис.1. Качественная схема грубого подслушивания

После разложения однофотонного волнового пакета в спектр, на траекториях, соответствующих частотам ω_1 и ω_2, подслушиватель в каждом измерении может "вставлять" на время ΔT (ожидаемое время срабатывания) фотодетекторы.

Если в линии присутствует один из узкополосных сигналов, то подслушиватель за время ожидания срабатывания ΔT с вероятностью $\Phi(\sigma\Delta T)$ регистрирует фотон и имеет информацию о данном бите в ключе. Если же в линии присутствует широкополосный сигнал, то может сработать любой из двух фотодетекторов. Вероятность срабатывания за время ожидания ΔT равна $P(\Delta T) = \sigma|f_\infty(\omega_{1,2})|^2\Phi(\sigma\Delta T) \approx (\sigma/\sigma_\infty)\Phi(\sigma\Delta T) \ll 1$.

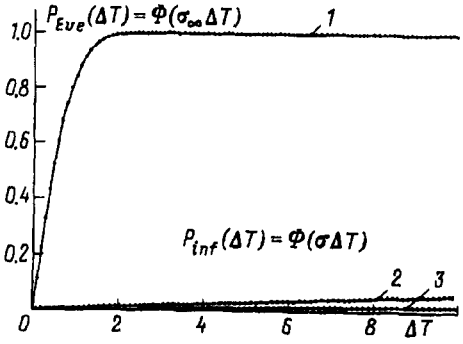

Рис.2.Вероятности обнаружения подслушивателя $P(\Delta T)_{eve} = (\sigma_\infty/\sigma)(\sigma/\sigma_\infty)\Phi(\sigma\Delta T)$ (кривая 1), где $N \sim \sigma_\infty/\sigma$. Кривые 2 и 3 – вероятности получения информации подслушивателем об одном бите в ключе $P_{inf}(\Delta T) \approx (\sigma/\sigma_\infty)\Phi(\sigma\Delta T)$. Отношение параметров σ/σ_∞ : 0.005; 0.001 для кривых 2 и 3, соответственно. Данное отношение параметров отвечает ширине спектра узкополосных $\sigma = 5\,\text{ns}^{-1}$; $1\,\text{ns}^{-1}$ и длительности широкополосного сигнала 1 ps

Вероятность детектирования широкополосного сигнала узкополосным фотодетектором мала: $p \approx \sigma/\sigma_\infty \ll 1$, соответственно вероятность не срабатывания $q \approx 1 - \sigma/\sigma_\infty$. Если имеется N посылок широкополосного сигнала, то вероятность регистрации в m опытах дается распределением Бернулли $P_m = C_N^m p^m q^{N-m}$. Вероятность регистрации хотя бы в одном из N опытов равна $P(N) = 1 - (1 - \frac{\sigma}{\sigma_\infty})^N$ и стремится к единице при $N \approx \sigma_\infty/\sigma$. Таким образом, если на N проверочных широкополосных сигналов посылается лишь один из узкополосных и подслушиватель в каждом измерении ожидает регистрации в течение времени ΔT, то вероятность обнаружения подслушивателя $P_{Eve}(N) = P(N)\Phi(\sigma_\infty \Delta T) \approx 1$. В то же время вероятность получения информации подслушивателем за время ожидания ΔT равна $P_{inf} = \Phi(\sigma\Delta T) \ll 1$. Графики зависимостей $\Phi(\sigma\Delta T)$ и $\Phi(\sigma_\infty \Delta T)$ для разных значений отношения σ/σ_∞ приведены на рис 2.

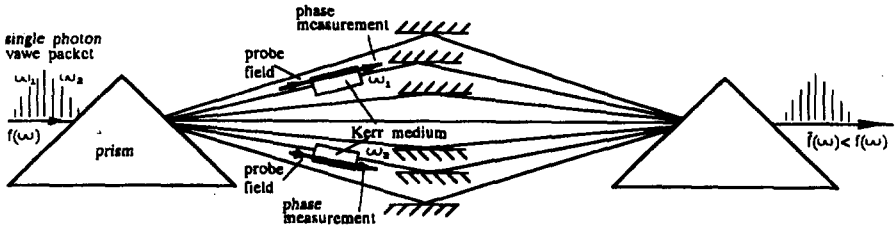

Рис.3. Качественная схема прозрачного подслушивания

Перейдем теперь к обсуждению стратегии прозрачного подслушивания. Схема измерения представлена на рис.3. После разложения в спектр каждая из монохроматических мод направляется в ячейку Керра (о применении ячеек Керра в неразрушающих измерениях см., например, [16]). Через ячейки Керра также пропускается вспомогательное пробное поле, над которым затем проводится измерение. Гамильтониан взаимодействия пробных полей с монохроматическими модами из однофотонного волнового пакета после прохождения призмы имеет вид

$$\hat{H} = \sum_i \chi_i^{(3)} \hat{N}_i \hat{n}_{\omega_i}, \qquad (7)$$

где $\chi_i^{(3)} = \chi_i^{(3)}(-\omega_i; \omega_i, -\omega_{pi}, \omega_{pi})$ – нелинейная восприимчивость третьего порядка, ω_{pi} и ω_i – частоты пробного поля и i-ой монохроматической составляющей однофотонного волнового пакета, $\hat{N}_i$ – оператор числа фотонов в i-пробном поле, и $\hat{n}_{\omega_i}$ – оператор числа фотонов в i-монохроматической однофотонной моде в волновом пакете. Совместная эволюция пробных полей и монохроматических мод в ячейках описывается оператором эволюции

$$\hat{U} = \exp\left(i \sum_k \chi_k \hat{N}_k \hat{n}_{\omega_k} \delta t_k\right), \tag{8}$$

где $\delta t_k = L_k / v_k$, v_k – скорость света в ячейке, L_k – длина ячейки, и $\tilde{\chi}_k = \chi_k^{(3)} L_k / v_k$. Пусть пробные поля описываются векторами состояний $|\Psi_k\rangle$; поскольку поля независимы, то общий вектор состояния есть

$$|\Psi\rangle = \prod_k |\Psi_k\rangle. \tag{9}$$

Действие оператора эволюции на состояния однофотонного волнового пакета и пробных полей сводится к следующему:

$$|\Phi\rangle = \hat{U}|1\rangle_f |\Psi\rangle = \sum_i f(\omega_i)|1_{\omega_i}\rangle \exp\left(i\tilde{\chi}_i \hat{N}_i\right) \prod_{j \neq i} |\Psi_j\rangle. \tag{10}$$

Пусть теперь подслушиватель и пользователь B проводят измерения при помощи проекционного оператора

$$\hat{P} = \left(\sum_i |1_{\omega_i}\rangle\langle 1_{\omega_i}|\right)(|\Psi\rangle\langle\Psi|). \tag{11}$$

Для B такое измерение означает использование широкополосного фотодетектора, а для подслушивателя измерение сводится к проектированию на исходное состояние пробных полей. Если пробные поля не "подцеплялись" к носителю ($\hat{U} \equiv 1$), то вероятность исходов измерений с $\hat{P}$ равна единице ($|\langle\Phi|\hat{P}|\Phi\rangle|^2 = 1$, поля с достоверностью находятся в исходном состоянии). Вероятность детектирования фотона пользователем B в каждом измерении также равна единице. Если же использовались ячейки Керра, то вероятность такого измерения

$$P = \sum_i |\tilde{f}(\omega_i)|^2 < 1, \quad \tilde{f}(\omega_i) = \langle\Psi_i| \exp\left(i\tilde{\chi}_i \hat{N}_i\right)|\Psi_i\rangle. \tag{12}$$

Формулу (12), по-видимому, можно интерпретировать как уменьшение вероятности детектирования фотона на приемном конце линии (см. также [17]).

Если в качестве пробного состояния использовать когерентное состояние

$$|\Psi_i\rangle = \exp\left(-|\alpha_i|^2/2\right) \sum_{k=0}^{\infty} \frac{\alpha_i^k}{\sqrt{k!}} |k\rangle, \tag{13}$$

где среднее число фотонов $\langle\hat{N}_i\rangle = |\alpha_i|^2$, то амплитуда однофотонного волнового пакета после измерения над пробным полем становится равной

$$|\tilde{f}(\omega_i)|^2 = |f(\omega_i)|^2 |\exp\left[(\exp(i\tilde{\chi} - 1))|\alpha_i|^2\right]| \approx |f(\omega_i)|^2 \exp\left(-\langle\hat{N}_i\rangle \tilde{\chi}_i^2/2\right) < |f(\omega_i)|^2. \tag{14}$$

В этой формуле для когерентного пробного поля уменьшение амплитуды лимитируется произведением в экспоненте $\langle N\rangle\tilde{\chi}^2$, которое не может быть меньше единицы [17–20]. Для других типов полей ситуация аналогичная [17–20]. Такое неизбежное уменьшение амплитуды следует из принципа дополнительности и является неизбежной платой за информацию о том, что фотон "проходил" по данной траектории (данная спектральная компонента отлична от нуля).

В случае широкополосного сигнала подслушиватель при прозрачной стратегии эффективно уменьшает амплитуду в интервале $\sim\sigma$ в районе спектральных компонент ω_1 и ω_2. Доля этих состояний в однофотонном пакете составляет величину порядка $\sim\sigma/\sigma_\infty \ll 1$. Вероятность "вырезания" части спектра при неразрушающем измерении подслушивателем в данном опыте не превышает $\delta\omega|f_\infty(\omega_{1,2})|^2|\langle\Psi|\exp(i\tilde{\chi}\hat{N})|\Psi\rangle|^2 \le (\sigma/\sigma_\infty) \ll 1$, где $\delta\omega \approx \sigma$. Поэтому вероятность обнаружить прозрачное подслушивание при посылке одного широкополосного сигнала мала и по порядку величины равна $\sigma/\sigma_\infty \ll 1$. Заметим, что для подслушивателя вероятность обнаружить изменение фазы пробного поля при измерении широкополосного сигнала также мала в меру малости $\delta\omega|f_\infty(\omega_{1,2})|^2$. Для обнаружения подслушивателя с вероятностью, близкой к единице, доля проверочных широкополосных сигналов по отношению к узкополосным, как и при грубом подслушивании, должна составлять $\sigma_\infty/\sigma \gg 1$.

В заключение выражаю благодарность Б.А.Волкову, С.В.Иорданскому, Г.Б.Лесовику, С.С.Назину, 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. W.K.Wotters and W.H.Zurek, Nature. **299**, 802 (1982).
2. C.Bennett, Phys. Rev. Lett. **68**, 3132 (1992); C.H.Bennett, G.Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
3. A.K.Ekert, B.Huttner, G.M.Palma, and A.Peres, Phys. Rev. **A50**, 1047 (1994).
4. C.H.Bennett, Tal Mor, and J.A.Smolin, *Parity Bit in Quantum Cryptography*, in http://xxx.lanl.gov/quant-ph/9604040.
5. E.Biham and Tal Mor, *On the Security of Quantum Cryptography against Collective Attack*, in http://xxx.lanl.gov/quant-ph/9605007.
6. Hoi-Kwong Lo and H.F.Chau, *Quantum Cryptography in Noisy Channels*, in http://xxx.lanl.gov/quant-ph/9511025.
7. С.Н.Молотков, С.С.Назин, Письма в ЖЭТФ **63**, 882 (1996); С.Н.Молотков, Письма в ЖЭТФ **64**, 652 (1996); также в http://xxx.lanl.gov/quant-ph/9612013; /9612012.
8. U.M.Titulaer and R.J.Glauber, Phys. Rev. **145**, 1041 (1966).
9. H.Fearn and R.Loudon, Opt. Commun. **64**, 485 (1987); H.Fearn, R.Loudon, J. Opt. Soc. Am. **B6**, 917 (1989).
10. R.A.Campos, B.E.Salech, and M.Teich, Phys. Rev. **A42**, 4127 (1990).
11. Н.Бор, Избранные научные труды, **2**, М.: Наука, (1971), с.675.
12. Л.И.Мандельштам, И.Е.Тамм, Известия АН СССР, сер. физ. **9**, N 1/2, 122 (1945).
13. Н.С.Крылов, В.А.Фок, ЖЭТФ **17**, 93 (1947); В.А.Фок, ЖЭТФ **42**, 1135 (1962).
14. В.В.Додонов, В.И.Манько, Труды ФИАН **183**, 52 (1987).
15. А.С.Холево, *Вероятностные и статистические аспекты квантовой теории*, М.: Наука, 1980.
16. N.Imoto, H.A.Haus, and Y.Yamamoto, Phys. Rev. **A32**, 2287 (1985); M.Kitagawa, N.Imoto, and Y.Yamamoto, Phys. Rev. **35**, 5270 (1987); I.L.Chuang, and Y.Yamamoto, Phys. Rev. Lett. **76**, 4281 (1996).
17. Z.Y.Ou, Phys. Rev. Lett. **77**, 2352 (1996).
18. C.W.Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, San Francisco, London, 1976.
19. R.Loudon, *The Quantum Theory of Light*, Clarendon Press, Oxford, 1973.
20. A.S.Lane, S.L.Braunstein, and C.M.Caves, Phys. Rev. **A47**, 1667 (1993).