Письма в ЖЭТФ, том 66, вып.1, стр.64 - 68 © 1997г. 10 июля

КВАНТОВАЯ КРИПТОГРАФИЯ НА ОСНОВЕ ГОМОДИННОГО ДЕТЕКТИРОВАНИЯ (КРИПТОСИСТЕМА НА ВАКУУМНОМ СОСТОЯНИИ)

С.Н.Молотков и С.С.Назин

Институт физики твердого тела РАН

142432 Черноголовка, Московская обл., Россия

Поступила в редакцию 3 июня 1997 г.

Предлагается новый протокол для квантовой криптографии, основанный на использовании набора измерений, позволяющих полностью восстанавливать матрицу плотности физической системы, являющейся носителем информации. В частности, такой протокол может быть реализован с помощью известного в квантовой оптике гомодинного детектирования электромагнитного поля. Приведен пример квантовой криптосистемы, в которой в качестве одного из двух информационных состояний используется вакуумное состояние фотонного поля.

PACS: 03.65.-w, 89.70.+c

Носителями информации в квантовой криптографии являются квантовые состояния. Информация извлекается в результате проведения тех или иных измерений над этими состояниями. Логическому нулю и единице отвечают посылки пользователем A пользователю B по квантовому каналу связи матриц плотности $\hat{\rho}_0 = |\psi_0\rangle\langle\psi_0|$ и $\hat{\rho}_1 = |\psi_1\rangle\langle\psi_1|$, соответственно (ниже мы ограничимся рассмотрением только чистых состояний). Секретность в квантовой криптографии базируется на том факте, что для пары неортогональных состояний невозможно получение какой бы то ни было информации без их возмущения [1, 2]. Точнее говоря, если заранее неизвестно, какое из двух неортогональных состояний подвергается измерению, то невозможно сделать достоверное (с вероятностью единица) утверждение о том, что это за состояние. В качестве носителей информации может быть использована любая пара неортогональных состояний [2]. В исходном протоколе генерации ключа [2] в канале без шума использовались операторы

$$\overline{P}_0 = 1 - |\psi_0\rangle\langle\psi_0| = 1 - \hat{\rho}_0, \quad \overline{P}_1 = 1 - |\psi_1\rangle\langle\psi_1| = 1 - \hat{\rho}_1. \tag{1}$$

Эти проекторы обладают очевидными свойствами:

$$\mathrm{Tr}\{\hat{\rho}_0\overline{P}_0\} \equiv 0, \quad \mathrm{Tr}\{\hat{\rho}_1\overline{P}_1\} \equiv 0. \tag{2}$$

При генерации ключа пользователями A и B, кроме квантового канала связи, используется также вспомогательный открытый (доступный всем) канал, по которому пользователь A сообщает пользователю B содержимое части посылок. Сопоставление пользователем B посланных состояний и полученных результатов измерений позволяет обнаруживать попытки подслушивания. Например, если пользователем A было послано состояние $\hat{\rho}_0$, а подслушивателем оно было интерпретировано (из-за невозможности достоверно отличить $\hat{\rho}_0$ от $\hat{\rho}_1$) как $\hat{\rho}_1$ и перепослано к B, то измерение над этим состоянием наблюдаемой, соответствующей проектору $\overline{P}_0$, может дать с вероятностью

$$\mathrm{Tr}\{\hat{\rho}_0\overline{P}_1\} = 1 - |\langle\psi_0|\psi_1\rangle|^2 \neq 0 \tag{3}$$

отличный от нуля результат. Этот результат является статистическим в том смысле, что гарантируется отличный от нуля результат на достаточно длинной серии измерений, хотя в каждом отдельном измерении можно получить и нулевой результат. В канале без шума достаточно первого ненулевого результата для обнаружения подслушивания. Однако этот "первый" ненулевой исход может иметь место не в первом измерении.

В реальных квантовых криптосистемах в качестве носителей информации до сих пор использовались фотонные состояния. Для них реализация экспериментальной процедуры измерения, отвечающей проекторам $\overline{P}_{0,1}$, является нетривиальной задачей. Наша идея состоит в том, чтобы отказаться от использования проекторов (1) при измерениях и вместо этого воспользоваться набором измерений M_θ, позволяющим по результатам большого числа измерений с различными θ полностью восстанавливать состояние квантовой системы. Так, в методе гомодинного детектирования электромагнитного поля, основанном на измерении квадратурной компоненты поля, используется следующее тождество для матрицы плотности поля [3–5]:

$$\hat{\rho} \equiv \int \frac{d^2\alpha}{\pi} \mathrm{Tr}\left\{\hat{\rho}\hat{D}^+(\alpha)\right\}\hat{D}(\alpha), \tag{4}$$

где $\hat{D}(\alpha) = \exp(-\alpha a^+ + \alpha^* a)$, a^+ и a – операторы рождения и уничтожения для соответствующей моды поля. При переходе к полярным координатам $\alpha = \frac{i}{2}k\exp(i\theta)$ формула (4) может быть переписана в виде

$$\hat{\rho} = \int_0^\pi \frac{d\theta}{\pi}\int_{-\infty}^{\infty}\frac{dk|k|}{4}\int_{-\infty}^{\infty} dx\ p(x,\theta)\exp(-ik(\hat{x}(\theta)-x)), \tag{5}$$

где $\hat{x}(\theta) = (a^+\exp(i\theta) + a\exp(-i\theta))/2$ – квадратурная переменная для фотонного поля, а угол θ представляет собой фазу пробного поля, которая задается измерительным устройством. След в (4) вычисляется в базисе собственных состояний квадратурной переменной $\{|x\rangle_\theta\}$, и $p(x,\theta) = {}_\theta\langle x|\hat{\rho}|x\rangle_\theta$. Плотность вероятности квадратурной компоненты $p(x,\theta)$ является экспериментально измеряемой величиной в методе гомодинной томографии [6]. Таким образом, величина $p(x,\theta)$ полностью определяет исходную матрицу плотности.

В предлагаемой криптосистеме протокол выглядит следующим образом. Пусть пользователь **A** посылает состояния $\hat{\rho}_0$ или $\hat{\rho}_1$ (0 или 1). Пользователь **B** случайно выбирает значение θ и проводит измерение M_θ. При этом он получает результат x (для простоты будем считать, что пространства результатов для всех измерений M_θ совпадают с множеством действительных чисел). После проведения серии измерений пользователь **A** для части измерений (например, половины) сообщает по открытому каналу пользователю **B** номера измерений, в которых было послано состояние $\hat{\rho}_0$. Пользователь **B** группирует свои данные в два массива. В одном присутствуют данные для тех номеров измерений, когда посылалось состояние $\hat{\rho}_0$, а в другом – данные для измерений, относящиеся к состоянию $\hat{\rho}_1$. Тогда достаточно длинная серия измерений даст пользователю **B** оценку для функций распределения $p_{0,1}(x,\theta)$ при фиксированном θ в состояниях $\hat{\rho}_0$ и $\hat{\rho}_1$. Точность этой оценки будет тем выше, чем длиннее проведенная серия измерений, и может быть получена из закона больших чисел.

Рассмотрим измерения, проведенные пользователем B над состоянием $\hat{\rho}_0$. Получаемые им в этом случае при заданном значении θ результаты x описываются случайной величиной ξ с плотностью вероятности $p_0(x,\theta)$ и соответствующей ей функцией распределения

$$P(x,\theta) = \Pr\{\xi \le x\} = \int_{-\infty}^{x} p(\xi,\theta)d\xi.$$

Пара (ξ, x) задает дискретную случайную величину ζ, принимающую значения 1 или 0 в зависимости от того, выполняется или нет неравенство $\xi \le x$. В реальных экспериментах число измерений всегда конечно; поэтому в распоряжении B имеется набор из N одинаковых независимых случайных величин ξ_i $(i = 1 \ldots N)$ при данном θ. Серия из N измерений задает случайную величину $P_N^*(x,\theta) = 1/N \sum_{i=1}^{N} \zeta_i$ с распределением

$$\Pr\{P_N^*(x,\theta) = \frac{k}{N}\} = \binom{N}{k} P(x,\theta)^k [1 - P(x,\theta)]^{N-k}. \qquad (6)$$

Если функция распределения $P(x,\theta)$ непрерывна, то мера отклонения эмпирической функции распределения от истинной дается теоремой Колмогорова [7, 8]:

$$\lim_{N\to\infty} \Pr\{\sqrt{N}\delta_N^+ \le z\} = \lim_{N\to\infty} \Pr\{\sqrt{N}\delta_N^- \le z\} = 1 - \exp(-2z^2) \qquad (7)$$

при любом z, и

$$\delta_N^{\pm} = \pm \sup_{-\infty<x<\infty} [P_N^*(x,\theta) - P(x,\theta)].$$

Таким образом, теорема Колмогорова позволяет указать границы, в которых сразу для всех значений аргумента с вероятностью, сколь угодно близкой к единице, заключена функция распределения $P_N^*(x,\theta)$. Если при некоторых N и z для открытой части измерений обнаружено, что одно из неравенств $\sqrt{N}\delta_N^+ \le z$ $\sqrt{N}\delta_N^- \le z$ нарушается, то это указывает на наличие подслушивания (обратное не верно).

Отметим, что и в протоколе [2] гипотеза об отсутствии подслушивания тоже должна приниматься по некоторому статистическому критерию. Действительно, допустим, что после обсуждения через открытый канал пользователь B выделил группу из N_0 проверочных измерений, в которых A посылал состояние $\hat{\rho}_0$, а B измерял наблюдаемую $\overline{P}_0$. Если подслушивания не было, то во всех N_0 измерениях должен быть получен нулевой результат. Однако если во всех измерениях имел место нулевой результат, то последнее вовсе не означает отсутствие подслушивания, так как имеется, хотя и небольшая, но все же отличная от нуля вероятность того, что подслушиватель правильно угадал посланное пользователем A состояние во всех проверочных посылках.

Остановимся теперь на секретности предлагаемого протокола. Для доказательства секретности необходимо показать, что не существует таких измерений, проводя которые подслушиватель мог бы по их результатам посылать пользователю B вместо перехваченных состояний другие матрицы плотности, подобранные так, что их смесь на состоянии $\hat{\rho}_0$ $(\hat{\rho}_1)$ окажется равной $\hat{\rho}_0$ $(\hat{\rho}_1)$. В нашем случае невозможность существования таких измерений очевидна, так как чистые состояния $\hat{\rho}_0$ и $\hat{\rho}_1$ являются крайними точками выпуклого пространства состояний квантовой системы, то есть не могут быть представлены в виде выпуклой линейной комбинации каких-либо других матриц плотности.

После того как установлено отсутствие подслушивания, оставшаяся нераскрытая часть измерений может служить для генерации ключа. Пользователь B может действовать следующим образом. Прежде всего ему необходимо выбрать некоторую решающую функцию $F_\theta^{\rho_0,\rho_1}(x)$, которая задает его стратегию интерпретации полученных результатов измерений: если в измерении, описываемом параметром θ, получен результат x, то пользователь B с вероятностью $F_\theta^{\rho_0,\rho_1}(x)$ выбирает логическую единицу и с вероятностью $1 - F_\theta^{\rho_0,\rho_1}(x)$ – логический нуль. Пусть $p_i(x,\theta)$ – вероятность получения результата x в измерении, описываемом параметром θ при условии того, что было послано состояние ρ_i. Заметим, что если состояния ρ_0 и ρ_1 посылаются пользователем A с равной вероятностью, то результат x будет наблюдаться в случае посылок состояния ρ_1 в $p_1(x,\theta)/p_0(x,\theta)$ раз чаще, чем в случае посылок состояния ρ_0. Поэтому естественно выбрать в качестве функции $F_\theta^{\rho_0,\rho_1}(x)$ величину, пропорциональную $p_1(x,\theta)$, то есть

$$F_\theta^{\rho_0,\rho_1}(x) = \frac{p_1(x,\theta)}{p_0(x,\theta) + p_1(x,\theta)}.$$

Для вычисления взаимной информации канала нужно найти вероятность $P(1,1)$ того, что при посылке пользователем A состояния ρ_1 пользователь B воспримет полученный в измерении результат как логическую единицу и соответствующую вероятность $P(0,0)$. Очевидно, что

$$P(1,1) = \int d\theta \Pi(\theta) \int dx F_\theta^{\rho_0,\rho_1}(x) p_1(x,\theta),$$

$$P(0,0) = \int d\theta \Pi(\theta) \int dx (1 - F_\theta^{\rho_0,\rho_1}(x)) p_0(x,\theta),$$

где $\Pi(\theta)$ – вероятность того, что пользователь B выбирает измерение, описывающееся параметром θ. Легко проверить, что $P(0,0) = P(1,1)$, то есть получающийся таким образом канал является симметричным. Поэтому, вводя обозначение $q = P(1,1) = P(0,0)$ (так что $P(0,1) = P(1,0) = 1 - q$), для искомой взаимной информации получаем

$$I = 1 + q \log_2 q + (1-q) \log_2 (1-q).$$

Согласно теореме Шеннона, I определяет информацию на одну посылку, которая может быть передана достоверно при помощи надлежащего блокового кода [9, 10].

Рассмотрим теперь вопрос о возможности практической реализации предлагаемой криптосистемы. Здесь можно воспользоваться упомянутым выше применяющимся в квантовой оптике гомодинным детектированием электромагнитного поля, позволяющим полностью восстанавливать его матрицу плотности по результатам некоторого набора измерений, параметризованного углом θ, представляющим собой фазу пробного поля [11]. В этом случае можно построить квантовую криптосистему на двух неортогональных состояниях, одно из которых является вакуумным состоянием электромагнитного поля $\hat{\rho}_0 = |0\rangle\langle 0|$, а второе – когерентное состояние поля, возникающее на выходе идеального лазера: $\hat{\rho}_1 = |\alpha\rangle\langle\alpha|$. При передаче логического нуля пользователь A ничего не

посылает в линию связи, а в случае логической единицы посылает когерентное состояние $|\alpha\rangle$. Когерентное состояние содержит вакуумную компоненту

$$|\alpha\rangle = \exp\left(-|\alpha|^2/2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle,$$

поэтому $\langle\alpha|0\rangle = \exp\left(-|\alpha|^2/2\right) \neq 0$; состояния тем больше неортогональны, чем меньше α (интенсивность когерентного излучения). Возможность восстановления матрицы плотности для вакуумного и сжатого состояний поля излучения была продемонстрирована экспериментально в работе [11]. Поэтому квантовая криптосистема с использованием вакуумного состояния представляется вполне реальной. Более того, она может оказаться даже проще в реализации, поскольку гомодинное детектирование не требует использования интерференционных эффектов на больших расстояниях, как это необходимо в существующих криптосистемах, основанных на интерферометрии с длинной базой (так называемый time division interferometer [12]).

Работа поддержана Российским фондом фундаментальных исследований (проект 96-02-19396).

---

1. W.K.Wootters and W.H.Zurek, Nature **299**, 802 (1982).
2. C.H.Bennett, Phys. Rev. Lett. **68**, 3132 (1992); C.H.Bennett, G.Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
3. K.E.Cahill and R.J.Glauber, Phys. Rev. **177**, 1882 (1969).
4. K.Vogel and H.Risken, Phys. Rev. **A40**, 2847 (1989).
5. G.M.D'Ariano, http://xxx.lanl.gov/quant-ph/9701011.
6. H.P.Yuen and J.H.Shapiro, IEEE Trans. Inf. Theory **IT–26**, 78 (1980); H.P.Yuen and V.W.S.Chan, Opt. Lett. **8**, 177 (1983).
7. A.N.Kolmogorov, Giornale dell'Instituto degli Attuari **4**, 83 (1933).
8. L.Takács, *Combinatorial Methods in the Theory of Stochastic Processes*, New York-London-Sydney: John Willey & Sons, Inc., 1967.
9. C.E.Shannon, *Mathematical Theory of Communications*, BSTJ **27**, 379; 623 (1948).
10. I.Csiszár and J.Körner, *Information Theory: Coding Theorems for Discreter Memoryless Systems*, Kiado–Budapest: Akademiai, 1981.
11. D.T.Smithey, M.Beck, M.G.Raymer, and A.Faridani, Phys. Rev. Lett. **70**, 1244 (1993).
12. C.Marand and P.D.Townsend, Optics Lett. **20**, 1695 (1995).