Письма в ЖЭТФ, том 66, вып.11, стр.736 - 741 © 1997г. 10 декабря

КВАНТОВАЯ КРИПТОГРАФИЯ НА КОГЕРЕНТНЫХ СОСТОЯНИЯХ НА ОСНОВЕ КВАНТОВОГО КОМПАРАТОРА

С.Н.Молотков

Институт физики твердого тела РАН

142432, Черноголовка, Московская обл., Россия

Поступила в редакцию 16 сентября 1997 г.

После переработки 28 октября 1997 г.

Предлагается квантовая криптосистема, основанная на сравнении входного сигнала из канала связи с реперным состоянием, приготовленным на приемном конце.

PACS: 03.65.-w, 89.70.+c

Квантовые криптосистемы в качестве носителей информации используют квантовые состояния. Секретность ключа в квантовой криптографии основывается на двух фактах – запрете клонирования (идеального копирования) заранее неизвестного квантового состояния [1] и невозможности получения любой информации о состояниях без их возмущения, если они неортогональны [2]. Протокол распространения ключа должен быть устроен так, чтобы измерения законных пользователей позволяли детектировать любые попытки подслушивания.

Идея предлагаемой квантовой криптосистемы основана на сравнении поступающего из канала связи состояния с реперным состоянием, приготовленным на приемном конце. Квантовая криптосистема на двух когерентных состояниях (одном опорном большой интенсивности и слабом информационном) обсуждалась в работе [3]. Существенное отличие предлагаемой системы от схемы [3] заключается в том, что в данном протоколе явно используется то обстоятельство, что когерентное излучение преобразуется светоделителем в себе подобное.

Всюду ниже канал связи предполагается идеальным.

Рассмотрим оптический светоделитель 50/50, рис.1. Пусть на входы светоделителя поступают два состояния поля, находящегося в когерентном состоянии. Когерентное состояние поля описывает излучение на выходе идеального лазера [4]. Состояние на входе светоделителя представляется в виде

$$|\psi\rangle_{in} = |\alpha\rangle_{in,a} \otimes |\beta\rangle_{in,b}, \quad \hat{\rho}_{in} = |\psi\rangle_{in}\ {}_{in}\langle\psi|, \tag{1}$$

где $|\alpha\rangle_{in}$ и $|\beta\rangle_{in}$ – когерентные состояния на входе оптического светоделителя. По определению последних, имеем

$$|\alpha\rangle_{in} = \hat{D}(\hat{a}_{in})|0\rangle_{in}, \quad \hat{D}(\hat{a}_{in}) = \exp\left(\alpha\hat{a}^{+}_{in} - \alpha^{*}\hat{a}_{in}\right); \tag{2}$$

здесь $\hat{D}(\hat{a}_{in})$ – оператор сдвига по группе когерентных состояний, $\hat{a}_{in}$ и $\hat{a}^{+}_{in}$ – операторы уничтожения и рождения для моды поля, $|0\rangle_{in}$ – вакуумное состояние для моды поля по входу a_{in}. Аналогично для входа b_{in}. Как известно [5], когерентное состояние является собственным состоянием оператора уничтожения

$$\hat{a}_{in}|\alpha\rangle_{in} = \alpha|\alpha\rangle_{in} \quad \text{и} \quad {}_{in}\langle\alpha|\hat{a}^{+}_{in} = {}_{in}\langle\alpha|\alpha^{*}, \tag{3}$$

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

где $|n\rangle$ – фоковское состояние с n фотонами. Любые два когерентных состояния, из-за присутствия в них вакуумной компоненты, неортогональны, даже если они имеют разные несущие частоты.

$$|_{in}\langle\beta|\alpha\rangle_{in}|^2 = \exp\left(-|\alpha - \beta|^2\right).$$

Светоделитель является унитарным преобразователем входных состояний поля в выходные, действие которого описывается унитарной матрицей 2×2; имеем

$$\begin{pmatrix} \hat{a}_{out} \\ \hat{b}_{out} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \hat{a}_{in} \\ \hat{b}_{in} \end{pmatrix} = \hat{U} \begin{pmatrix} \hat{a}_{in} \\ \hat{b}_{in} \end{pmatrix}. \tag{4}$$

Такой подход, при котором оптическая схема преобразует операторы поля, а сами состояния остаются неизменными, соответствует гейзенберговской картине. Возможен другой подход (шредингеровское представление), когда оптический тракт преобразует состояния поля, а не операторы [6].

Операторы чисел фотонов на выходах светоделителя равны

$$\hat{a}^+_{out}\hat{a}_{out} = \left(\frac{\hat{a}^+_{in} - \hat{b}^+_{in}}{\sqrt{2}}\right)\left(\frac{\hat{a}_{in} - \hat{b}_{in}}{\sqrt{2}}\right), \tag{5}$$

$$\hat{b}^+_{out}\hat{b}_{out} = \left(\frac{\hat{a}^+_{in} + \hat{b}^+_{in}}{\sqrt{2}}\right)\left(\frac{\hat{a}_{in} + \hat{b}_{in}}{\sqrt{2}}\right).$$

Среднее число фотонов на выходах a и b с учетом (3) и (5), соответственно, равно (ниже подразумевается, что несущие частоты у входных состояний одинаковы)

$$N_{a,out} = \mathrm{Tr}\{\hat{\rho}_{in}\hat{a}^+_{out}\hat{a}_{out}\} = |\frac{\alpha - \beta}{\sqrt{2}}|^2, \tag{6}$$

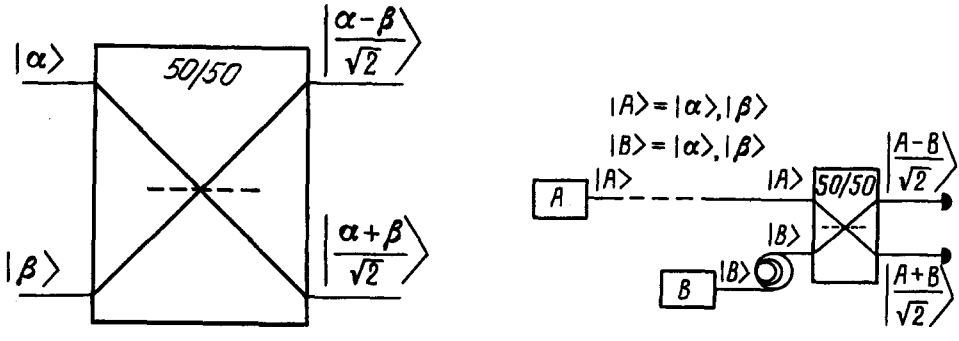
$$N_{b,out} = \mathrm{Tr}\{\hat{\rho}_{in}\hat{b}^+_{out}\hat{b}_{out}\} = |\frac{\alpha + \beta}{\sqrt{2}}|^2.$$

Таким образом, для входных сигналов в *когерентном состоянии* (*и только для них*) светоделитель работает как квантовый компаратор. Если входные состояния совпадают, то на одном из выходов ("вычитающем") происходит полная компенсация сигналов – полная деструктивная интерференция. На "суммирующем" выходе в этом случае имеет место полная конструктивная интерференция.

При совпадении состояний на входах вероятность зарегистрировать фотон на "вычитающем" выходе фотодетектора *тождественно* равна нулю, поскольку состояние "вычитающего" выхода отвечает вакуумному состоянию, которое является *собственным состоянием* оператора числа фотонов с собственным значением $N_{a,out} = 0$. Если состояния на входах светоделителя не совпадают, то выходные состояния на выходах $|\frac{\alpha-\beta}{\sqrt{2}}\rangle_{a,out}$ и $|\frac{\alpha+\beta}{\sqrt{2}}\rangle_{b,out}$ *не являются собственными состояниями* оператора числа квантов. Последнее физически означает, что $N_{a,out}$ и $N_{b,out}$ являются *средним* числом квантов, регистрируемых фотодетектором по большой серии измерений. В каждом отдельном измерении (при несовпадении сигналов на входах) может быть

зарегистрировано любое число квантов на каждом из выходов. В силу этого, неизбежны будут события, когда на "вычитающем" выходе не будет срабатывания фотодетектора (зарегистрировано нуль квантов). Причем, доля таких событий будет тем больше, чем ближе разность $\alpha-\beta$ к нулю (чем состояния ближе друг к другу или, что то же самое, чем они более неортогональны). Поэтому, если на "вычитающем" выходе не произошло срабатывания фотодетектора, то это событие не позволяет сделать определенного заключения о втором входном состоянии при известном реперном (так называемый inconclusive result). В то же время, если известно, какое состояние должно быть на втором входе и если оно совпадало с реперным, то срабытывание фотодетектора на "вычитающем" выходе дает *однозначное* заключение о том, что состояние на втором входе было изменено подслушивателем.

Резюмируя, приходим к заключению, что если сработали одновременно оба детектора, то это событие означает, что реперное состояние не совпадает с пробным. Но если сработал только нижний детектор, то нельзя сделать определенного вывода о пробном состоянии. По-существу данное обстоятельство (которое является следствием неортогональности состояний) приводит к тому, что подслушиватель будет неизбежно ошибаться.



Обсудим теперь применение данного квантового компаратора для распространения ключа (случайной последовательности 0 и 1) между двумя пользователями. Принципиальная схема квантовой криптосистемы представлена на рис.2. Пользователи A и B имеют два идентичных источника, которые могут приготавливать по выбору состояния $|\alpha\rangle_{in}$ или $|\beta\rangle_{in}$ ($\alpha \neq \beta$). Кроме того, у пользователя B имеется линия задержки, равная длине линии связи. Предполагается, что часы у пользователей в каждой посылке синхронизированы. Протокол генерации ключа выглядит следующим образом.

Пользователи A и B случайно и независимо друг от друга приготавливают состояния $|\alpha\rangle_{in}$ и $|\beta\rangle_{in}$, отвечающие логическому нулю или единице.

После проведения серии посылок, для части из них через открытый канал связи пользователь A сообщает номера тех измерений, когда было послано $|\alpha\rangle_{in}$, а когда – $|\beta\rangle_{in}$. Пользователь B проверяет исходы измерений, когда посылка от A совпадала с его реперным состоянием. Если подслушивание отсутствует, то для этих измерений на "вычитающем" выходе компаратора должен иметь место нулевой исход. Первый ненулевой исход при идеальном канале связи указывает на наличие подслушивателя.

После того как установлен факт отсутствия подслушивания, оставшаяся часть измерений служит для генерации секретного ключа. Для этого пользователь B сооб-

щает номера тех измерений, для которых имеет место ненулевой результат на обоих выходах компаратора, но не сообщает, какое реперное состояние при этом он использовал ($|\alpha\rangle_{in}$ или $|\beta\rangle_{in}$). Этой информации достаточно для пользователей, чтобы иметь идентичный секретный ключ. Действительно, если в данном измерении имел место ненулевой исход на обоих выходах и, например, пользователь B использовал в качестве реперного состояние $|\alpha\rangle_{in}$ (логический нуль), то это могло иметь место только тогда, когда пользователь A посылал состояние $|\beta\rangle_{in}$, и наоборот. В этом случае пользователи принимают в ключ логический нуль. Аналогично для логической единицы. В результате возникает идентичная и секретная последовательность нулей и единиц.

В последнее время были предложены различные варианты протоколов обмена для квантовых криптосистем [2,3,7–13]. Однако экспериментально реализованы лишь системы [14–17], которые основываются на протоколе, предложенном в работе [2]. Эти системы представляют собой достаточно сложный интерферометр с разделением по времени (так называемый time division interferometer [14–17]), в котором для обеспечения секретности требуется ослабление сигнала до уровня одного фотона в импульсе. В реальных экспериментах [14–17] ослабление излучения происходит до уровня $0.1 \div 0.2$ фотона в посылке.

На наш взгляд, главная трудность при реализации состоит в следующем. Формально для реализации квантовой криптосистемы достаточно иметь в качестве носителей любую пару неортогональных состояний [2], например, $|u_0\rangle$ и $|u_1\rangle$, и измерительное "устройство", которое реализует действие проекторов $\overline{P}_0 = 1 - |u_0\rangle\langle u_0|$ и $\overline{P}_1 = 1 - |u_1\rangle\langle u_1|$. Измерения с данными проекторами позволяют обнаружить *любые* изменения состояний $|u_0\rangle$ и $|u_1\rangle$, что гарантирует секретность криптосистемы. Однако нет никакого общего рецепта, который бы позволял по написанному проектору предъявить экспериментальное устройство, его реализующее. Особенно сложно реализовать проекторы, если они не отвечают никакой физической наблюдаемой.

Когерентное излучение лазера наиболее удобно для использования в качестве носителей информации, например $|\alpha\rangle$ и $|\beta\rangle$ (неортогональность $|\alpha\rangle$ и $|\beta\rangle$ имеет место при $\alpha \neq \beta$, что достигается просто изменением интенсивности излучения в разных посылках). Однако достаточно сложно реализовать проектор "отрицания" для когерентного состояния $\overline{P}(\alpha) = 1 - |\alpha\rangle\langle\alpha|$ и $\overline{P}(\beta) = 1 - |\beta\rangle\langle\beta|$. Известно лишь, как реализовать проекторно-значную меру для когерентного состояния $\hat{M}(d\alpha) = |\alpha\rangle\langle\alpha| d^2\alpha/\pi$ при помощи достаточно тонкой методики гомодинного детектирования [18], но отнюдь не проектор $\overline{P}(\alpha)$. Причем, такая проекторно-значная мера реализуется для идеального гомодинного детектирования, когда фаза опорного сигнала ("локального осциллятора") строго задана, что достигается формально лишь при бесконечной интенсивности опорного сигнала.

Фактически по этой причине приходиться ослаблять интенсивность сигнала до однофотонного уровня. Если в сигнале присутствует только одно фоковское состояние $|n\rangle$ ($n = 1$), то проектор на такое состояние реализуется достаточно просто при помощи обычного фотодетектора. Если $n > 1$, то пока не существует фотодетекторов, которые бы позволяли отличать состояния с разными числами фотонов. Кроме того, в экспериментах (см. детали в [14–17]) однофотонное состояние получается путем сильного ослабления лазерного излучения, то есть сигнал имеет вид

$|\alpha\rangle \approx |0\rangle + \alpha|1\rangle + \ldots$ (при $\alpha \ll 1$) [17]. Поэтому, строго говоря, требуется реализация проектора на такое состояние, что не дает обычный фотодетектор.

Кроме того, имеется еще одна неприятность с использованием ослабленного до однофотонного уровня лазерного излучения. Такое ослабление в принципе не может дать никакой гарантии, что в посылке присутствует один, а не два или более фотонов. Конечно, вероятность присутствия n фотонов убывает по мере уменьшения α. Присутствие более чем одного фотона в посылке может быть использовано для подслушивания путем "отвода" части фотонов. Причем такие попытки не детектируются в реализации [14–17].

В предлагаемой схеме, на наш взгляд, отсутствуют упомянутые трудности именно потому, что схема действует как квантовый компаратор (производит "вычитание" аргументов во входных когерентных состояниях по одному из каналов и "сложение" по второму – $|\alpha\rangle \otimes |\beta\rangle \rightarrow |\frac{\alpha-\beta}{\sqrt{2}}\rangle \otimes |\frac{\alpha+\beta}{\sqrt{2}}\rangle$). На окончательном этапе измерения при помощи фотодетектора производится измерение наблюдаемой $N_{a,out} = \mathrm{Tr}\{\hat{\rho}_{in}\hat{a}^{+}_{out}\hat{a}_{out}\}$ и $N_{b,out} = \mathrm{Tr}\{\hat{\rho}_{in}\hat{b}^{+}_{out}\hat{b}_{out}\}$ – числа квантов в уже преобразованных компаратором состояниях $|\frac{\alpha-\beta}{\sqrt{2}}\rangle$ и $|\frac{\alpha+\beta}{\sqrt{2}}\rangle$, а не проекторов $\mathrm{Tr}\{\hat{\rho}\overline{P}(\alpha)\}$ и $\mathrm{Tr}\{\hat{\rho}\overline{P}(\beta)\}$. Причем, для протокола не требуется отличать события с разным числом квантов, достаточно лишь факта регистрации или не регистрации. Не требуется также ослабления лазерного излучения до однофотонного уровня, можно использовать сигналы любой интенсивности. Хотя не существует формального запрета на интерференцию от двух независимых источников при их идеальной синхронизации, однако при экспериментальной реализации данное обстоятельсво может представлять заметные трудности (так же, как и при реализации схемы [3]).

На наш взгляд, существенная разница данной схемы по сравнению с другими состоит в том, что в данной схеме явно используется тот факт, что когерентное состояние не разрушается светоделителем (остается на выходе когерентным, но с другим параметром). Использование этого нетривиального, но хорошо известного в квантовой оптике свойства когерентного излучения, которое в других работах по квантовой криптографии ранее не использовалось, можно надеяться, упростит экспериментальную реализацию квантовых криптосистем. Другие состояния поля не переводятся светоделителем в себе подобные, что означает невозможность квантового компаратора на светоделителе для произвольных состояний излучения, в том числе и однофотонного.

Выражаю благодарность С.В.Иорданскому, В.Ф.Клюеву и С.С.Назину за полезные обсуждения в процессе выполнения работы. Работа поддержана Российским фондом фундаментальных исследований (проект 96-02-18918), а также грантом 110/57/1–3 программы "Перспективные технологии в микро- и наноэлектронике".

---

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. B.Huttner, N.Imoto, N.Gisin, and T.Mor, Phys. Rev. **A51**, 1863 (1995).
4. Ф.Ареки, М.Скалли, Г.Хакен, В.Вайдлих, *Квантовые флуктуации излучения лазера*, М.: "Мир", 1974 (перевод: *Quantum Optics*, Ed. R.J.Glauber, New York: Academic Press, 1969).
5. В.В.Додонов, В.И.Манько, *Инварианты и эволюция нестационарных квантовых систем*, Труды ФИАН **183** (1987).
6. Д.Н.Клышко, УФН **164**, 1187 (1994).

7. A.K.Ekert, Phys. Rev. Lett. **67**, 661 (1991).
8. A.K.Ekert, J.G.Rarity, P.R.Tapster, and G.M.Palma, Phys. Rev. Lett. **69**, 1293 (1992).
9. L.Goldenberg and L.Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
10. M.Koashi and N.Imoto, Phys. Rev. Lett. **77**, 2137 (1996).
11. E.Biham, B.Huttner, and T.Mor, Phys. Rev. **A54**, 2651 (1996).
12. A.Muller, J.Brequet, and N.Gisin, Europhys. Lett. **30**, 809 (1994).
13. M.Koashi and N.Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
14. C.Marand and P.D.Townsend, Optics Lett. **20**, 1695 (1995).
15. R.J.Hughes, D.M.Alde, P.Dyer et al., Contemp. Phys. **36**, 149 (1995).
16. S.J.D.Phoenix and P.D.Townsend, Contemp. Phys. **36**, 165 (1995).
17. A.Muller, T.Herzog, B.Huttner et al., Appl. Phys. Lett. **70**, 793 (1997).
18. 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).