Письма в ЖЭТФ, том 66, вып.11, стр.742 - 745

КВАНТОВАЯ КРИПТОГРАФИЯ НА НЕСТАЦИОНАРНЫХ СОСТОЯНИЯХ

С.Н.Молотков, С.С.Назин

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, в которой в качестве носителей информации используется пара нестационарных состояний, отличающихся моментом приготовления.

PACS: 03.65.-w, 89.70.+c

Секретность квантовых криптосистем основывается на невозможности в общем случае достоверного различения с помощью одного измерения двух состояний ρ_0 и ρ_1 (например, двух неортогональных чистых состояний), используемых для кодирования информации [1]. При этом протокол генерации ключа для двух пользователей A и B выбирается таким образом, чтобы измерений, проводимых обоими пользователями (или одним из них), было достаточно для обнаружения подслушивателя в квантовом канале связи между A и B. Так, в предложенной в работе [2] квантовой криптосистеме используется пара чистых неортогональных квантовых состояний $|u_0\rangle$ и $|u_1\rangle$ (им отвечают матрицы плотности $\rho_{0,1} = |u_{0,1}\rangle\langle u_{0,1}|$). В схеме [2] используются два измерения, которым отвечают проекторы $\overline{P}_0 = 1 - P_0$ и $\overline{P}_1 = 1 - P_1$, где $P_{0,1} = |u_{0,1}\rangle\langle u_{0,1}| \equiv \rho_{0,1}$. Проекторы $\overline{P}_{0,1}$ проектируют на подпространства, ортогональные $|u_0\rangle$ и $|u_1\rangle$, соответственно; поэтому

$$\mathrm{Tr}\{\overline{P}_0\hat{\rho}_0\} = 0, \quad \mathrm{Tr}\{\overline{P}_1\hat{\rho}_1\} = 0, \tag{1}$$

$$\mathrm{Tr}\{\overline{P}_{0,1}\hat{\rho}_{1,0}\} = 1 - |\langle u_0|u_1\rangle|^2 \neq 0, \quad \hat{\rho}_{0,1} = |u_{0,1}\rangle\langle u_{0,1}|.$$

Измерения проекторами $\overline{P}_{0,1}$ позволяют обнаружить любые изменения чистых состояний $|u_0\rangle$ и $|u_1\rangle$ в проверочных посылках, когда обоим пользователям известно, какое состояние было послано [2]. При этом неявно подразумевается, что состояния $|u_0\rangle$ и $|u_1\rangle$ являются стационарными, так как в противном случае их временная эволюция привела бы к необходимости в различные моменты времени t_m проводить измерения, соответствующие различным проекторам $\overline{P}_{0,1}(t_m) = 1 - |u_{0,1}(t_m)\rangle\langle u_{0,1}(t_m)|$. Отметим также, что требование неортогональности состояний $|u_0\rangle$ и $|u_1\rangle$ приводит к тому, что эти состояния должны иметь одну и ту же энергию. В противном случае стационарные состояния с разной энергией были бы автоматически ортогональны.

В этой статье мы хотим на примере простейшей квантовой системы показать, как можно построить квантовую криптосистему на нестационарных состояниях, основанную на измерении наблюдаемой времени; при этом необходимые измерения могут производиться пользователем B в любой фиксированный, выбранный им, момент времени.

Рассмотрим двухуровневую систему с не зависящим от времени гамильтонианом H, диагонализуемым в базисе $|e_0\rangle$, $|e_1\rangle$ (энергии $E_0 = 0$ и $E_1 = \omega$; считаем, что

$\hbar = 1$). По аналогии со случаем непрерывного спектра [3] рассмотрим разложение единицы на интервале $[0, T)$ $(T = 2\pi/\omega)$:

$$M(d\tau) = \frac{d\tau}{T} \sum_{k,l=0,1} |e_k\rangle\langle e_l| \exp i(E_k - E_l)\tau, \tag{2}$$

которое соответствует ковариантному измерению наблюдаемой времени τ. Ограничение $0 \leq \tau < T$ связано с тем, что любое состояние невозмущенной двухуровневой системы периодично во времени с периодом T. Разложение единицы (2) удобно переписать в виде

$$M(d\tau) = (\sigma_0 + \sigma_1 \cos\omega\tau + \sigma_2 \sin\omega\tau)\frac{d\tau}{T}, \tag{3}$$

где σ_i $(i = 1,\ 2,\ 3)$ – матрицы Паули, а σ_0 – единичная матрица 2×2.

Допустим теперь, что в распоряжении пользователя A имеются два, отличающиеся только моментом приготовления, состояния ρ_0 и ρ_1 (не обязательно чистые; излагаемая ниже схема в равной мере применима для чистых и смешанных состояний), которые он по квантовому каналу связи отправляет пользователю B, то есть

$$\rho_i(t) = e^{-iH(t-t_i)}\rho_g e^{iH(t-t_i)}, \quad i = 0, 1; \quad 0 \leq t_0 < t_1 < T, \tag{4}$$

где ρ_g – некоторое фиксированное "порождающее" состояние. Воспользуемся для ρ_i представлением

$$\rho_i(t) = \frac{1}{2}(\sigma_0 + v_i^k(t)\sigma_k), \tag{5}$$

где v^k – компоненты некоторого вектора $|\mathbf{v}| \leq 1$, то есть $((v^1)^2 + (v^2)^2 + (v^3)^2)^{1/2} \leq$ ≤ 1. Эволюция вектора $\mathbf{v}$ в случае невозмущенной системы определяется уравнением $\dot\rho = i[\rho, H]$ с $H = \omega(\sigma_0 - \sigma_3)/2$ и соответствует прецессии вектора $\mathbf{v}$ вокруг оси z с частотой ω.

Теперь ясно, что вероятность получения результата в интервале $(\tau, \tau + d\tau)$ при измерении $M(d\tau)$, проведенном над состоянием ρ в момент времени t_m, есть

$$P_M(\tau)d\tau = \mathrm{Tr}(\rho M(d\tau)) = (1 + v^1(t_m)\cos\omega\tau + v^2(t_m)\sin\omega\tau)\frac{d\tau}{T}. \tag{6}$$

Таким образом, функция распределения $P_M(\tau)$ является суммой постоянной величины $1/T$ и линейной комбинации $v^1(t_m)\cos\omega\tau + v^2(t_m)\sin\omega\tau$. Зная функцию распределения $P_M(\tau)$, можно легко определить коэффициенты $v^1(t_m)$ и $v^2(t_m)$ при косинусе и синусе, установив таким образом два из трех параметров, задающих матрицу плотности системы. Кроме того, измерение энергии получаемых пользователем состояний (то есть измерение наблюдаемой, соответствующей гамильтониану H) дает результаты 0 и ω с вероятностями $P = (1 \pm v^3)/2$ (формально измерению энергии соответствует разложение единицы $M(d\epsilon)$ на прямой, сосредоточенное в двух точках – 0 и ω). Таким образом, знание полной статистики измерений $M(d\tau)$ и $M(d\epsilon)$ позволяет полностью восстановить состояние ρ. Этим обстоятельством можно воспользоваться для обнаружения подслушивателя в квантовом канале связи, по которому пользователь A передает пользователю B состояния ρ_0 и ρ_1. Действительно, если состояния ρ_0 и ρ_1 таковы, что их нельзя с достоверностью различить в одном измерении (например, если они соответствуют двум неортогональным чистым состояниям, когда $|\mathbf{v}_i| = 1$), то можно предложить следующий протокол генерации ключа.

Пусть вся ось времени разбита на равные интервалы продолжительностью T (мы предполагаем, что часы у пользователей синхронизованы) и в каждый из этих интервалов пользователь A случайным образом приготавливает и посылает пользователю B одно из состояний ρ_0 или ρ_1 (в каждой посылке параметры t_0 и t_1 отсчитываются от начала соответствующего интервала). Пользователь B независимо от A случайно выбирает тип проводимого им измерения – $M(dt)$ или $M(d\epsilon)$ (в некоторый фиксированный, то есть одинаковый для всех посылок момент времени t_m). Результатом измерения являются τ с вероятностью $P_M(\rho; d\tau)$ в первом случае или энергия E (принимающая значения из множества $\{0, \omega\}$) с вероятностью $P(\rho; E)$. Как обычно, считается, что параметры t_0, t_1 и порождающее состояние ρ_g заранее известны всем, включая подслушивателя, но неизвестно, что будет послано пользователем A в каждой конкретной посылке – ρ_0 или ρ_1. Наличие в канале связи подслушивателя обнаруживается следующим образом. После достаточно длинной серии измерений пользователь A для части измерений (например, половины) сообщает, в каких случаях он посылал ρ_0, а в каких – ρ_1. Среди этих посылок пользователь B рассматривает только те, в которых посылалось состояние ρ_0 и он проводил измерения $M(d\tau)$; пусть число таких измерений есть N. Затем он выбирает произвольное $0 \leq \theta < T$ и подсчитывает число случаев N_θ, когда в результате измерения были получены значения $\tau \leq \theta$. Введем теперь функцию распределения $F(\tau) = \int_0^\tau d\tau' P_M(\tau')$ (по которой так же, как и по $P_M(\tau)$ однозначно восстанавливаются параметры v^1 и v^2 матрицы плотности) и случайную величину ξ, которая равна единице, если полученное в данном измерении значение $\tau \leq \theta$, и нулю в противоположном случае. Тогда из неравенства Чебышева для суммы N экземпляров независимых случайных величин $\xi_k - p$, где $p = F(\theta)$, следует, что для любого ϵ

$$\Pr\left\{\left|\frac{N_\theta}{N} - p\right| \geq \epsilon\right\} \leq \frac{p(1-p)}{N\epsilon^2} \leq \frac{1}{4N\epsilon^2}. \tag{7}$$

Таким образом, при $N \to \infty$ вероятность отклонения эмпирической функции распределения $F_N(\theta) = N_\theta/N$ от заранее известной функции распределения $F(\theta)$ равномерно по θ стремится к нулю как N^{-1}. Зафиксировав некоторое достаточно малое значение ϵ_0, пользователь B может считать, что в канале связи присутствует подслушиватель, если хотя бы при одном θ неравенство $|N_\theta/N - p| \leq \epsilon_0$ оказывается нарушенным. Действительно, поскольку по функции $F(\tau)$ однозначно восстанавливаются параметры v^1 и v^2 матрицы плотности, отклонение $F_N(\tau)$ от $F(\tau)$ говорит о том, что измерения, выполненные пользователем B, проводились над состояниями, у которых по крайней мере один из параметров v^1 или v^2 отличен от соответствующего параметра $\rho_0(t_m)$. Аналогичная процедура может быть применена к анализу распределения результатов измерения энергии для случаев, когда посылались состояния ρ_0, что позволяет выявить отклонение параметра v^3 от $v_0^3(t_m)$. Поскольку параметры $v^{1,2,3}$ полностью задают состояние рассматриваемой двухуровневой системы, описанная процедура позволяет обнаружить любую попытку подслушивателя подменить посылаемое пользователем A состояние.

После установления отсутствия подслушивания с заданной вероятностью в распоряжении у пользователя B остается набор измерений $M(d\tau)$. Измерения $M(d\tau)$ в каждой отдельной попытке из-за неортогональности состояний ρ_0 и ρ_1 не позволяют достоверно отличать 0 от 1. Достоверная информация о секретном ключе (последовательности 0 и 1), остающаяся у пользователей в результате применения, например, случайного блокового кода, составляет величину, меньшую одного бита на каждую посылку. Эта величина описывается взаимной информацией, которая в нашем случае дается формулой для симметричного бинарного канала [4, 5]:

$$I = 1 + q\log_2 q + (1 - q)\mathrm{loq}_2(1 - q), \tag{8}$$

где q – вероятность ошибки, то есть $q = P(1|0) = P(0|1)$ – условная вероятность того, что был послан 0, который при приеме был интерпретирован как 1, и наоборот. Соответственно вероятность правильной интерпретации есть $1-q = P(1|1) = P(0|0)$. Конкретные значения величин $P(i|j)$ определяются выбранной пользователем B стратегией интерпретации полученных им результатов измерения $M(d\tau)$.

Выражаем благодарность С.В.Иорданскому и В.Ф.Клюеву за полезные обсуждения в процессе выполнения работы. Работа поддержана Российским фондом фундаментальных исследований (проект 96-02-19396).

---

1. W.K.Wootters, 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. А.С.Холево, *Вероятностные и статистические аспекты квантовой теории*, М.: Наука, 1980.
4. C.E.Shannon, BSTJ **27**, 379; 623 (1948).
5. I.Csiszár, J.Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Kiado–Budapest: Akademiai, 1981.