Московский Физико-Технический Институт
(Государственный Университет)

Факультет общей и прикладной физики
Кафедра "Проблемы теоретической физики"

Квалификационная выпускная работа на соискание степени магистра

студента 928 группы Баяндина К.В.

Использование многокубитных запутанных квантовых состояний для передачи зашифрованных сообщений.

Научный руководитель:
д.ф.м.н. Лесовик Г.Б.

Москва
2005

Содержание

Введение

В 1982 году Фейнман предположил, что одна квантовая система может моделировать другую лучше, чем классические компьютеры, которые требуют экспоненциальных затрат вычислительных ресурсов в зависимости от размеров моделируемой системы [1]. Позже внимание общественности было привлечено к возможности использования квантово-механических систем для решения классических задач. Например, алгоритм Дойча [2] по определению сбалансированности целочисленной функции был первым квантовым алгоритмом, который работал эффективнее классического аналога.

Наиболее известный из всех, квантовый алгоритм Шора [3], разлагающий составные целые числа на множители, способен разрушить распространенную криптографическую систему RSA [4]. Этот факт произвел большое впечатление на научное сообщество, и ускорил развитие квантовой криптографии [5] и теории квантовой информации в целом.

Важно отметить, что квантовая механика, разрушая классические способы шифрования, дает возможность для создания новых. На данный момент существует несколько различных способов шифрования, которые используют квантовую механику.

Одним из примеров является квантовый алгоритм разделения секретного ключа, основанный на использовании ортогональных состояний фотонов [6]. Он был впервые экспериментально реализован Беннетом и Брассардом [7], которые были способны производить секретную передачу сообщений на расстояние всего лишь 40 сантиметров. Позже, была реализована линия связи длиной несколько километров [8].

Другой метод был экспериментально реализован в 1992 году [9], для этого использовались пары запутанных фотонов, часть из которых, благодаря неравенствам Клаузера-Хорна [10], могла быть использована, для того чтобы выявить попытки подслушивания.

В данной работе предложен другой способ шифрования. В нем используется квантовый компьютер для создания запутанных состояний нескольких кубитов. Защищенность этого способа шифрования основана на сложности томографии таких состояний.

В дальнейшем будет удобно рассматривать отдельный кубит, как частицу со спином $\frac{1}{2}$. Чтобы отправить информацию, Алиса (отправитель) сначала записывает ее в виде последовательности битов - нулей и единиц, разделяя их на группы по K битов. Потом, для каждой группы, она создает набор из K спинов в чистых состояниях. Каждый спин, соответствующий определенному биту, получает проекцию вдоль фиксированной оси Z, если бит равен нулю, и проекцию против оси - в другом случае. После этого Алиса производит некоторое унитарное преобразование $\hat{U}$ для каждой группы из K спинов, тем самым получая множество запутанных квантовых состояний, которые в дальнейшем будут называться сообщениями:

$$|\Psi_k\rangle = \hat{U}|k\rangle, \tag{1}$$

где $|k\rangle$ - это незапутанное состояние спинов с определенными проекциями вдоль оси Z, причем проекции спинов определяются последовательностью нулей и единиц в двоичной записи числа k.

Получив K запутанных спинов очередного сообщения, Боб (получатель) производит обратное преобразование $\hat{U}^{-1}$, тем самым получая начальное незапутанное состояние спинов с определенными проекциями, которые могут быть измерены, и, соответственно, секретное сообщение будет расшифровано.

Предполагается, что только Алиса и Боб знают унитарное преобразование $\hat{U}$, тогда Ева (взломщик), пытаясь провести измерение над запутанными состояниями, будет получать вероятностные результаты, определяемые квантовой механикой.

В дальнейшем мы будем рассматривать способы, при помощи которых Ева может расшифровать передаваемую информацию, и, самое главное, как много времени это займет. Мы будем рассматривать два разных способа: квантовую томографию запутанного состояния в первой главе и простой подбор сети квантовых вентилей, реализующих унитарное преобразование $\hat{U}$, во второй главе. В четвертой главе мы рассмотрим пример, как квантовая томография может быть реализована для спиновых состояний электронов в мезоскопической системе. Полученные результаты позволят оценить, как долго Алиса и Боб могут безопасно использовать унитарное преобразование, не изменяя его.

1 Квантовая томография запутанного состояния.

В самом простом случае Ева может определить секретное унитарное преобразование, если она перехватит большое количество сообщений, и о каждом из них она будет знать исходную последовательность битов. Мы оставим вопрос о том, как Ева может узнать такую информацию. Мы лишь будем предполагать в этой главе, что в распоряжении Евы есть большое количество идентичных запутанных состояний.

Стратегия Евы состоит в том, чтобы применять квантовую томографию для большого количества идентичных запутанных состояний. В работе [11] было показано, что матрица плотности квантово-механического состояния нескольких спинов может быть получена даже без использования квантового компьютера. Идея метода основана на измерении вероятности $p(\vec{n}_1, m_1; ...; \vec{n}_K, m_K)$ для каждого спина $\hat{s}_i$ спроецированного в состояние m_i вдоль направления $\vec{n}_i$. Матрица плотности вычисляется при помощи интегрирования по методу Монте-Карло:

$$\hat{\rho}_{calc} = \sum_{\{m_i\}=-\frac{1}{2}}^{\frac{1}{2}} \int \frac{d\vec{n}_1 ... d\vec{n}_K}{(4\pi)^K} p(\vec{n}_1, m_1; ...; \vec{n}_K, m_K) \hat{K}_{S_1}(m_1 - \vec{s}_1\vec{n}_1) ... \hat{K}_{S_K}(m_K - \vec{s}_K\vec{n}_K), \quad (2)$$

где ядро интегрирования:

$$\hat{K}_{S_i}(m_i - \vec{s}_i\vec{n}_i) = \frac{2}{\pi} \int_0^{2\pi} d\psi \sin^2 \frac{\psi}{2} e^{i\psi(m_i - \vec{s}_i\vec{n}_i)} \quad (3)$$

действует только в гильбертовом пространстве i-го спина.

Введем меру длины для матриц плотности:

$$|\hat{\rho}_1, \hat{\rho}_2| = \sqrt{\sum_{i,j} |\hat{\rho}_1 - \hat{\rho}_2|^2_{ij}}, \qquad |\hat{\rho}| = \sqrt{\sum_{i,j} |\hat{\rho}|^2_{ij}}. \quad (4)$$

Общеизвестно, что в методе Монте-Карло относительная точность интегрирования сходится к истинному значению как обратный корень от числа использованных точек [12]. В нашем случае мы имеем:

$$\alpha = \frac{|\hat{\rho}_{calc} - \hat{\rho}_{true}|}{|\hat{\rho}_{true}|} \approx \frac{1}{\sqrt{N}}, \tag{5}$$

где N - это число различных наборов направлений, использованных для измерений спинов.

Заметим, что для каждого фиксированного набора направлений, вдоль которых измеряются спины, необходимо измерить вероятности для всех комбинаций индексов $\{m_i\}$. Это требует около $Const * 2^K$ перехваченных сообщений.

Тем самым, мы получаем, что для того чтобы определить матрицу плотности с точностью α, необходимо перехватить:

$$N_{intercepted} \approx Const * \alpha^{-2} * 2^K \tag{6}$$

сообщений.

Для того, чтобы получить желаемое унитарное преобразование, Ева должна определить матрицы плотности $\{\rho_k\}$ для всех 2^K запутанных состояний. Каждая матрица плотности $\{\rho_k\}$ имеет единственное собственное значение 1, и единственный собственный вектор $|\Psi_k\rangle$:

$$\hat{\rho}_k = |\Psi_k\rangle\langle\Psi_k|. \tag{7}$$

Еве необходимо найти собственные вектора 2^K матриц плотности для всех запутанных состояний, а затем сложить в матрицу коэффициенты разложения $\{C_{ik}\}$ этих состояний в некотором базисе:

$$|\Psi_k\rangle = \sum_{i=0}^{2^K-1} C_{ik}|i\rangle, \tag{8}$$

тем самым она получит матрицу $2^K \times 2^K$ для унитарного преобразования $\hat{U}$ в базисе векторов $|k\rangle$. Так как проблема нахождения собственных векторов матрицы требует порядка 2^{2K} элементарных операций, все вычисление займет около:

$$N_{operations} = 2^{3K} \tag{9}$$

элементарных операций, предполагая, что в распоряжении Евы имеется квантовый компьютер, способный оперировать

$$N_{data} = 2^{2K} \tag{10}$$

комплексными числами.

В довершение ко всему, Ева должна сконструировать сеть из элементарных квантовых вентилей по унитарному преобразованию. Как это будет ясно в дальнейшем, число необходимых вентилей будет порядка:

$$N_{gates} \approx 2^{2K}. \tag{11}$$

Итак, по мере того, как Алиса и Боб увеличивают число битов содержащихся в одиночном сообщении, число перехваченных сообщений, время, необходимое для определения унитарного преобразования, и сложность создаваемой квантовой сети растет экспоненциально.

2 Подбор унитарного преобразования.

Ева вместо того, чтобы определять структуру запутанных состояний и унитарного преобразования, может попытаться подобрать обратное унитарное преобразование на своем квантовом компьютере. Сложное унитарное преобразование может быть составлено из простых преобразований - базовых вентилей. Наиболее активно изучаемые вентили для квантовых сетей основаны на сверхпроводящих контурах [13], резонансных полостях [14], линейных ионных ловушках [15] и ядерном магнитном резонансе [16].

Работа квантового компьютера может быть представлена в виде последовательного выполнения простых унитарных преобразований. В таком случае полное унитарное преобразование имеет вид:

$$\hat{U} = \hat{U}_M \hat{U}_{M-1} ... \hat{U}_2 \hat{U}_1, \tag{12}$$

здесь каждое из унитарных преобразований $\left\{\hat{U}_i\right\}$ действует лишь в пространстве нескольких кубитов, причем среди них могут быть одинаковые преобразования.

Экерт и Джоза показали [17], что любое преобразование нескольких кубитов может быть получено последовательным выполнением простых: всевозможных однокубитных и любого фиксированного нетривиального двухкубитного преобразования. Примером такого двухкубитного преобразования может служить "контролируемое-НЕ", действие которого описывается как $|a, b\rangle \rightarrow |a, a \oplus b\rangle$.

Так как для каждого простого унитарного преобразования существует обратное ему ("контролируемое-НЕ"обратно к самому себе), то легко можно составить обратное унитарное преобразование:

$$\hat{U}^{-1} = \hat{U}_1^{-1} \hat{U}_2^{-1} ... \hat{U}_{M-1}^{-1} \hat{U}_M^{-1} .. \tag{13}$$

Хотя авторами [17] и был приведен алгоритм, позволяющий построить квантовую сеть вентилей по любому унитарному преобразованию, в общем случае для этого требуется полиномиальное число базовых вентилей в зависимости от размерности матрицы $\hat{U}$. Тем самым, в нашем случае, для этого потребуется число вентилей экспоненциальное по количеству кубитов. Однако, Алиса и Боб не нуждаются в построении квантового компьютера, реализующего произвольное унитарное преобразование, вместо этого они могут договориться использовать конкретную квантовую сеть вентилей.

Мы предполагаем, что Алиса и Боб располагают одинаковыми квантовыми компьютерами, которые могут выполнять какие либо из L фиксированных унитарных преобразований, предполагая, что в среди них для каждого существует обратное. Если Алиса и Боб используют унитарные преобразования из этого набора M раз, то число всевозможных квантовых сетей оценивается величиной:

$$N_{quant}(L, M) = L^M. \tag{14}$$

Ева не имеет никаких шансов угадать правильное унитарное преобразование, пробуя все возможные квантовые сети. Дело в том, что Алиса и Боб при помощи своего унитарного преобразования $\hat{U}$ должны смешать состояния каждого кубита с

каждым, то есть числа M и L должны быть не меньше K^2. Как видно, зависимость (14) опять экспоненциальная. В этой формуле еще не учтен тот факт, что для каждой пробной квантовой сети Ева должна провести несколько измерений квантово-механических состояний, что бы убедиться, что данная сеть реализует верное унитарное преобразование. Пусть

$$p = |\langle k|\hat{U}_{guess}^{-1}\hat{U}|k\rangle|^2 \tag{15}$$

это вероятность ошибочного принятия пробного унитарного преобразования $\hat{U}_{guess}$ вместо верного $\hat{U}$. Тогда вероятность не отличить эти два преобразования за n измерений, будет:

$$P = p^n = e^{n \ln p}. \tag{16}$$

Поскольку, для подавляющего большинства квантовых сетей, вероятность p много меньше единицы, то будет достаточно провести несколько измерений для одного пробного унитарного преобразования, чтобы выяснить, угадано оно или нет.

В результате мы получили, что для увеличения безопасности предлагаемого криптографического метода, Алиса и Боб должны увеличивать не только число используемых кубитов, но и число используемых квантовых вентилей.

3 Случай априорно известных временных корреляций.

Ранее мы предполагали, что Ева знает, какая именно информация зашифрована в виде запутанных состояний. В этой главе предполагается, что она знает лишь временные корреляции между сообщениями состоящими из K классических битов. Корреляции определяются формулой:

$$\xi_{kl}(y) = \langle p_k(x) p_l(x+y)\rangle_x, \tag{17}$$

где $p_k(x)$ равняется единице, если x-ое сообщение записывается как $|k\rangle$, и ноль в противном случае. Среднее считается по большому набору равноотстоящих друг от друга сообщений.

Мы предполагаем, что Ева обладает априорной информацией, такой как частоты появления и корреляции между сообщениями посылаемыми Алисой. Стратегия Евы в этом случае заключается в том, чтобы настроить свой квантовый компьютер так, чтобы у расшифрованных им сообщений были такие же частоты появления и временные корреляции.

Оценка количества перехваченных сообщений, необходимых, чтобы вывести унитарное преобразование, получается произведением: числа пробных унитарных преобразований и числа необходимых измерений для каждого из них, чтобы определить, подходящие получаются корреляции или нет. Первая часть проблемы определяется квантово-механической запутанностью состояний, а вторая аналогична случаю классического шифра замены.

Число пробных унитарных преобразований определяется формулой (14). Для определения корреляций между перехваченными сообщениями необходимо измерить

такое число квантовых состояний, которое полиномиально по величине 2^K

$$N_{cl} \approx P_n\left(2^K\right), \tag{18}$$

где степень n полинома $P_n(x)$ соответствует порядку учитываемых корреляций. Например, в формуле (17) написана корреляция второго порядка. Для корреляций n-го порядка необходимо усреднять произведение из n величин $p_k(x)$.

Окончательная формула для числа сообщений, которые Еве необходимо перехватить:

$$N_{net} \approx N_{quant} * N_{cl}. \tag{19}$$

4 Возможная реализация квантовой томографии в мезоскопической системе.

4.1 Использование корреляторов электрических токов для изучения структуры запутанных квантово-механических состояний.

В последние годы идет интенсивное изучение основ квантовой механики и феномена квантовой запутанности в применении к квазичастицам в мезоскопических системах. Некоторое время назад, по аналогии с оптическими экспериментами по изучению запутанных пар фотонов, было предложено использовать сверхпроводник, как источник запутанных пар квазичастиц [18], происходящих из одной куперовской пары. Позднее были предложены неравенства типа Белла [19] для корреляторов электрических токов. Эти неравенства справедливы для классических теорий скрытых локальных параметров, но квантовая-механика позволяет нарушить эти неравенства при некоторых специфических обстоятельствах. Тем самым, появилась возможность в очередной раз убедиться в том, что экспериментально измеримые вероятности предсказываемые квантовой механикой - это не результат присутствия неких скрытых переменных, а фундаментальная особенность окружающего мира.

В этих [18], [19] и последующих работах в неравенствах Белла использовались кросс-корреляторы двух электрических токов на нулевой частоте. Эти неравенства не дают какой либо дополнительной информации о том, какая имеется структура у квантово-механических состояний двух электронов распространяющихся по различным проводникам; то, насколько они нарушаются, может лишь указывать степень запутанности этих электронов [22].

В этой главе мы хотим показать, как можно использовать корреляторы электрических токов на конечных временах для определения структуры квантово-механического состояния. Мы оставим в стороне вопрос о том, как можно получить многокубитные состояния спинов электронов на практике, пока это теоретически описано всего лишь для пар электронов [19]. В данный момент нас интересует поведение Евы, которая много раз перехватывает по K электронов, спиновое состояние которых является зашифрованным сообщением.

Предположим, что по K баллистическим проводникам распространяются K электронов, спины которых находятся в состоянии описываемом матрицей плотности ρ. Пусть каждый проводник нумеруется индексом i, а каждая группа из K электронов - индексом j. Пусть в i-м проводнике электрон пересекает некоторое сечение в моменты времени: $t_j + \tau_i$, здесь t_j - это моменты времени, в которые Ева перехватывает j группу по K электронов, а τ_i - это смещение электронов по времени внутри каждой из групп (первый электрон имеет нулевое смещение: $\tau_1 = 0$). Если предположить, что в каждой группе смещения электронов друг относительно друга одни и те же, то измерение коррелятора K электрических токов будет иметь максимум на следующих временах:

$$\left\langle \hat{I}_1(t_1)\hat{I}_2(t_2)...\hat{I}_K(t_K) \right\rangle \sim \delta_{\tau_{wp}}(t_2 - t_1 - \tau_2)\delta_{\tau_{wp}}(t_3 - t_1 - \tau_3)...\delta_{\tau_{wp}}(t_K - t_1 - \tau_K), \qquad (20)$$

здесь мы воспользовались тем, что в стационарном режиме коррелятор токов зависит только от разности времен, и использовали обозначение дельта-функции с шириной τ_{wp} равной ширине волнового пакета электрона.

Теперь, чтобы воспользоваться формулой (2) Еве необходимо уметь производить "опыт Штерна-Герлаха"для каждого отдельного электрона, то есть отбирать только те группы по K электронов, спиновые состояния которых проектируются вдоль направлений $\vec{n}_i$ - по одному для каждого электрона.

В теоретических работах обсуждается возможность создания спиновых фильтров на основе гетероструктур ферромагнетик-нормальный металл или двух квантовых точек с сильной спин-орбитальной связью [20], есть даже экспериментальные работы по измерению спинового состояния электронов [21], но до широкого распространения таких приборов еще далеко.

Однако, предположим, что Ева способна сконструировать достаточно хорошие спиновые фильтры, которые разделяют электроны согласно проекций их спинов вдоль заданных направлений. Тогда коррелятор электрических токов после фильтрования будет иметь вид:

$$\left\langle \hat{I}_1(t_1)\hat{I}_2(t_2)...\hat{I}_K(t_K) \right\rangle_{filt} \sim p(\vec{n}_1, +\frac{1}{2}; ...; \vec{n}_K, +\frac{1}{2}) \left\langle \hat{I}_1(t_1)\hat{I}_2(t_2)...\hat{I}_K(t_K) \right\rangle , , \qquad (21)$$

здесь $p(\vec{n}_1, +\frac{1}{2}; ...; \vec{n}_K, +\frac{1}{2})$ - это вероятность для спинов электронов спроектироваться вдоль выбранных направлений.

По двум величинами (20) и (21) можно посчитать искомые вероятности для большого числа направлений, и численно проинтегрировать (2). Конечно же, чем точнее будут измерены эти вероятности, тем точнее будет восстановлена искомая матрица плотности.

Далее, в этой главе, мы последовательно рассмотрим задачу об экспериментальном измерении корреляторов электрических токов, которая может быть интересна сама по себе.

4.2 Измерение корреляторов в квантовой механике.

Согласно общей теории измерений, мы рассматриваем ситуацию, когда вся квантовая система состоит из системы-измерителя с некоторой наблюдаемой $\hat{x}$, имеющей

определенные собственные значения и собственные вектора, и резервуаров (в нашем случае это квантовые проводники с электронами). В таком случае корреляции электрических токов в резервуарах будут изучаться через корреляции $\left\langle \hat{x}(t_1)\hat{x}(t_2) \right\rangle$ для системы-измерителя.

Все гильбертово пространство H системы может быть представлено в виде прямого произведения пространства H_m системы-измерителя и пространства H_e резервуаров, так что: $H = H_m \otimes H_e$. Мы предполагаем, что взаимодействие между системами описывается гамильтонианом взаимодействия:

$$\hat{H}_I(t) = \sum_i \alpha_i \hat{x} \hat{I}_i(t), \tag{22}$$

где оператор $\hat{x}$ действует только в гильбертовом пространстве системы-измерителя, в то время, как операторы токов $\hat{I}_i$ действуют в пространствах резервуаров с электронами.

В гильбертовом пространстве системы-измерителя мы можем ввести базис из полного набора собственных векторов оператора $\hat{x}$: $\hat{x}|x_n\rangle = x_n|x_n\rangle$. Пусть A' - это такое событие, что в момент времени t_1 измерение величины $\hat{x}$ дало x_n, тогда как A - это такое событие, что измерение в момент времени t_2 привело к результату x_m. В таком случае корреляционная функция для этих двух событий будет записана как:

$$\left\langle \hat{x}(t_1)\hat{x}(t_2) \right\rangle = \sum_{n,m} x_n x_m P_A(x_m, t_2|x_n, t_1) P_{A'}(x_n, t_1), \tag{23}$$

где $P_{A'}(x_n, t_1)$ - это вероятность получить собственное значение x_n в момент времени t_1 и $P_A(x_m, t_2|x_n, t_1)$ - это условная вероятность получить собственное значение x_m в момент времени t_2, если в момент времени t_1 была получена величина x_n.

Позже, в этой главе, мы будем работать в представлении взаимодействия, так что

$$|x_n(t)\rangle = e^{\frac{i}{\hbar}\hat{H}_0 t}|x_n\rangle, \tag{24}$$

$$\hat{x}(t) = e^{\frac{i}{\hbar}\hat{H}_0 t}\hat{x}e^{-\frac{i}{\hbar}\hat{H}_0 t}, \tag{25}$$

$$|x_n(t_2)\rangle = \hat{S}(t_2, t_1)|x_n(t_1)\rangle, \tag{26}$$

$$\hat{\rho}(t) = \hat{S}(t, -\infty)\hat{\rho}(-\infty)\hat{S}^\dagger(t, -\infty), \tag{27}$$

где $\hat{H}_0$ - это гамильтониан системы-измерителя без взаимодействия с резервуаром, $\hat{S}(t_2, t_1)$ - это оператор эволюции от момента времени t_1 до t_2, записанный в представлении взаимодействия. Как обычно, мы считаем, что взаимодействие выключено при бесконечно отрицательных временах, а потом оно адиабатически включается, соответственно $\hat{\rho}(-\infty)$ - это матрица плотности всей системы в начальный момент времени, когда взаимодействие было выключено.

В квантовой механике вероятность $P(x_n, t_1)$ может быть записана как след от произведения матрицы плотности $\hat{\rho}$ и проектора $\hat{P}_n(t) = |x_n(t)\rangle\langle x_n(t)|$:

$$P(x_n, t_1) = \mathrm{Tr}\hat{\rho}(t_1)\hat{P}_n(t_1). \tag{28}$$

Согласно постулату фон Неймана, после первого измерения в момент времени t_1 матрица плотности редуцируется:

$$\hat{\rho}(t_1) \to \hat{\rho}_1(t_1) = |x_n(t_1)\rangle \frac{\langle x_n(t_1)|\hat{\rho}(t_1)|x_n(t_1)\rangle}{\mathrm{Tr}_{el}\langle x_n(t_1)|\hat{\rho}(t_1)|x_n(t_1)\rangle} \langle x_n(t_1)|, \tag{29}$$

здесь числитель дроби - это матрица в гильбертовом пространстве H_e электронных резервуаров, а Tr_{el} - это след по индексам в нем. Знаменатель необходимо написать для того, чтобы выполнялось условие нормировки $\mathrm{Tr}\hat{\rho}_1 = 1$.

В таком случае условная вероятность измерить x_m в момент времени $t_2 > t_1$ может быть записана как:

$$P(x_m, t_2|x_n, t_1) = \mathrm{Tr}\hat{\rho}_1(t_2)\hat{P}_m(t_2), \tag{30}$$

где $\hat{\rho}_1(t_2)$ - это матрица плотности всей системы, которая унитарно эволюционировала с момента времени t_1 до момента времени t_2:

$$\hat{\rho}_1(t_2) = \hat{S}(t_2 - t_1)\hat{\rho}_1(t_1)\hat{S}^{+}(t_2 - t_1), \tag{31}$$

где $\hat{S}(t_2 - t_1)$ - это оператор эволюции с момента времени t_1 до момента времени t_2.

Согласно (28), (29) и (30), используя перестановочные свойства следа Tr, мы получаем:

$$\left\langle \hat{x}(t_1)\hat{x}(t_2) \right\rangle = \mathrm{Tr}\left[\hat{S}(t_2, t_1) D\left\{ \hat{S}(t_1, -\infty)\hat{\rho}(-\infty)\hat{S}^{\dagger}(t_1, -\infty)\hat{x}(t_1) \right\}_{t_1} \hat{S}^{\dagger}(t_2, t_1)\hat{x}(t_2) \right], \tag{32}$$

где мы использовали тот факт, что $\hat{x}(t) = \sum\limits_n |x_n(t)\rangle x_n \langle x_n(t)|$ и мы ввели обозначение для проекционного измерения:

$$D\left\{\hat{A}(t)\right\}_t = \sum_n |x_n(t)\rangle\langle x_n(t)|\hat{A}(t)|x_n(t)\rangle\langle x_n(t)|. \tag{33}$$

Эта величина (32) будет измеряться в реальном эксперименте, и желаемые корреляторы появятся из зависимости матрицы плотности и оператора эволюции от изучаемых токов.

4.3 Механический осциллятор, как измеритель корреляций ток-ток.

В работах [25], [26] изучался вопрос измерения автокорреляций электрического тока при помощи LC-контура и механического осциллятора. Подобным же образом можно описать процесс измерения кросс-корреляций электрических токов, и в обоих случаях системой-измерителем будет квантовый осциллятор. В случае изучения автокорреляций, при помощи LC-контура с малым затуханием, в выражение вида (32) в правую часть вошла спектральная плотность шума на собственной частоте колебательного контура. В случае использования механического осциллятора для измерения тока, изучались автокорреляции тока на конечных временах больших, чем время затухания колебаний осциллятора.

Рассмотрим последовательное квантово-механическое описание процесса измерения кросс-коррелятора двух электрических токов при помощи обыкновенного амперметра, который представляет из себя механический осциллятор, и является системой-измерителем. Стрелка амперметра является частью осциллятора, а угол ее отклонения - его координатой.

Гамильтониан такой системы имеет вид:

$$\hat{H} = \hat{H}_{el} + \hat{H}_{osc} + \hat{H}_{int}, \tag{34}$$

где $\hat{H}_{el}$ - это гамильтониан электронов в резервуаре, гамильтониан механического осциллятора:

$$\hat{H_{osc}} = \frac{1}{2}(\hat{\dot{x}}^2 + \omega_0^2 \hat{x}^2), \tag{35}$$

а гамильтониан взаимодействия:

$$\hat{H}_I = \hat{x}\left(\alpha_1 \hat{I}_1 + \alpha_2 \hat{I}_2\right), \tag{36}$$

где α_i - это константы взаимодействия осциллятора с изучаемыми токами. Сейчас мы описываем один осциллятор, который является системой-измерителем. В этом случае, вычисления во многом похожи на вычисления для автокорреляций одного тока.

Оператор эволюции в представлении взаимодействия записывается в виде:

$$\hat{S}(t_2, t_1) = T \exp\left[-\frac{i}{\hbar}\int\limits_{t_1}^{t_2} dt' \hat{H}_I(t')\right]. \tag{37}$$

Мы используем разложение оператора эволюции по константам взаимодействия:

$$\hat{S}(t_2 - t_1) \approx 1 + \left(-\frac{i}{\hbar}\right)\int\limits_{t_1}^{t_2} dt' \hat{H}_I(t') + ... \tag{38}$$

Подставляя (38) в (32) и оставляя только квадратичные члены по константам взаимодействия, можно получить:

$$\left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle = \left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_0 + \sum_{k=1}^{2}\sum_{l=1}^{2}\left(-\tfrac{i}{\hbar}\right)^2 \alpha_k' \alpha_l' \tag{39}$$

$$\left(\int\limits_{t_1}^{t_2} dt' \int\limits_{t_1}^{t'} dt''\left(-[\hat{x}(t'')\hat{x}(t_2)]\left\langle D\{\hat{x}(t_1)\hat{x}(t')\}_{t_1}\right\rangle \left\langle \hat{I}_l(t'')\hat{I}_k(t')\right\rangle^A + [\hat{x}(t')\hat{x}(t_2)]\left\langle\langle\hat{x}(t_1)\hat{x}(t'')\rangle\right\rangle \left\langle \hat{I}_l(t'')\hat{I}_k(t')\right\rangle^A\right) + \right. \tag{40}$$

$$\int\limits_{-\infty}^{t_1} dt' \int\limits_{-\infty}^{t'} dt''\Big[[\hat{x}(t')\hat{x}(t_2)]\Big(\left\langle[\hat{x}(t'')\hat{x}(t_2)]\right\rangle \left\langle \hat{I}_l(t'')\hat{I}_k(t')\right\rangle^S + \left\langle\{\hat{x}(t'')\hat{x}(t_2)\}\right\rangle \left\langle \hat{I}_l(t'')\hat{I}_k(t')\right\rangle^A\Big) + \tag{41}$$

$$[\hat{x}(t')\hat{x}(t_1)]\Big(\left\langle[\hat{x}(t'')\hat{x}(t_1)]\right\rangle \left\langle \hat{I}_l(t'')\hat{I}_k(t')\right\rangle^S + \left\langle\{\hat{x}(t'')\hat{x}(t_1)\}\right\rangle \left\langle \hat{I}_l(t'')\hat{I}_k(t')\right\rangle^A\Big)\Big] +$$

$$\left.\int\limits_{-\infty}^{t_1} dt' \int\limits_{t_1}^{t_2} dt''[\hat{x}(t'')\hat{x}(t_2)]\Big(\left\langle[\hat{x}(t')\hat{x}(t_1)]\right\rangle \left\langle \hat{I}_l(t')\hat{I}_k(t'')\right\rangle^S + \left\langle\{\hat{x}(t')\hat{x}(t_1)\}\right\rangle \left\langle \hat{I}_l(t')\hat{I}_k(t'')\right\rangle^A\Big)\right), \tag{42}$$

где $\left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_0$ - это корреляционная функция механического осциллятора без взаимодействия с электрическими токами; здесь мы ввели обозначение для скобок

коммутатора и антикоммутатора: $\left[\hat{A}\hat{B}\right] = \hat{A}\hat{B} - \hat{B}\hat{A}$ и $\left\{\hat{A}\hat{B}\right\} = \hat{A}\hat{B} + \hat{B}\hat{A}$, и использовали факт, что для осциллятора без затухания: $[\hat{x}(t_1)\hat{x}(t_2)]$ - это с-число, так что мы можем вынести его из под скобок усреднения по матрице плотности.

Для корреляций ток-ток мы использовали обозначение:

$$\left\langle \hat{I}_l(t_1)\hat{I}_k(t_2)\right\rangle^S = \frac{1}{2}\left\langle \hat{I}_l(t_1)\hat{I}_k(t_2) + \hat{I}_k(t_2)\hat{I}_l(t_1)\right\rangle,\ t_1 < t_2 \tag{43}$$

$$\left\langle \hat{I}_l(t_1)\hat{I}_k(t_2)\right\rangle^A = \frac{1}{2}\left\langle \hat{I}_l(t_1)\hat{I}_k(t_2) - \hat{I}_k(t_2)\hat{I}_l(t_1)\right\rangle,\ t_1 < t_2. \tag{44}$$

В реальной ситуации осциллятора с затуханием мы заменяем коммутаторы их средними, посчитанными по формуле Кубо:

$$\left\langle \hat{x}(t_1)\hat{y}(t_2) - \hat{y}(t_2)\hat{x}(t_1)\right\rangle = i\hbar\alpha_{xy}(t_2 - t_1), \tag{45}$$

и средние от антикоммутаторов считаются согласно Флуктуационно-Диссипативной теореме:

$$\left\langle \hat{x}(t_1)\hat{y}(t_2) + \hat{y}(t_2)\hat{x}(t_1)\right\rangle = 2\hbar \int\limits_{-\infty}^{\infty} \alpha''_{xy}(\omega) cth\frac{\hbar\omega}{2T} e^{-i\omega(t_2-t_1)}\frac{d\omega}{2\pi}, \tag{46}$$

где T - это температура осциллятора, $\alpha(t)$, $t > 0$ - это линейный отклик, а $\alpha(\omega) = \alpha'(\omega) + i\alpha''(\omega)$ - это обобщенная восприимчивость осциллятора. Эти величины считаются из классических уравнений движения:

$$\ddot{x} + \gamma\dot{x} + \omega_0^2 x = f_\omega e^{-i\omega t}, \tag{47}$$

$$\alpha_{xx}(\omega) = \frac{1}{\omega_0^2 - \omega^2 - i\gamma\omega}, \quad \alpha_{xx}(t) = e^{-\frac{\gamma}{2}t}\frac{\sin\Omega t}{\Omega}, \tag{48}$$

где $\Omega = \sqrt{\omega_0^2 - \gamma^2/4}$ - это резонансная частота осциллятора при учете затухания.

В следствие того, что коммутаторы и антикоммутаторы пропорциональны $e^{-\frac{\gamma}{2}t}$, удобно рассматривать случай, когда временные масштабы изменения электрических токов τ_{el} много больше, чем обратная величина затухания γ^{-1} для осциллятора. Это довольно логичное предположение, так как колебания стрелки амперметра должны успокоиться прежде, чем изменятся электрические токи. В таком случае мы интересуемся временами: $(t_2 - t_1) \sim \tau_{el} \gg \gamma^{-1}$. Согласно нашим оценкам, останется лишь член (42), а все остальные исчезнут при интегрировании.

Используя тот факт, что электрические токи не меняются на масштабах γ^{-1}, мы можем вынести корреляторы ток-ток из под интегрирования:

$$\int\limits_{-\infty}^{t_1} dt' \left\langle [\hat{x}(t')\hat{x}(t_1)]\right\rangle I(t') = i\hbar\frac{1}{\omega_0^2} I(t_1), \tag{49}$$

$$\int\limits_{-\infty}^{t_1} dt' \left\langle \{\hat{x}(t')\hat{x}(t_1)\}\right\rangle I(t') = \hbar\frac{\gamma^2}{\omega_0^4}\frac{2T}{\hbar\gamma} I(t_1), \tag{50}$$

Для члена отвечающего за кросс-корреляции мы получим

$$\left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle = \left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_0 + \sum_{k=1}^{2}\sum_{l=1}^{2}\frac{\alpha_k\alpha_l}{\omega_0^4}\left\{\left\langle \hat{I}_k(t_1)\hat{I}_l(t_2)\right\rangle^S - i\left\langle \hat{I}_k(t_1)\hat{I}_l(t_2)\right\rangle^A\left(\frac{\gamma^2}{\omega_0^2}\frac{2T}{\hbar\gamma}\right)\right\} + ... \tag{51}$$

где мы использовали старые обозначения для (43) и (44). В правую часть выражение (51) входят как кросс-корреляции, так и автокорреляции токов, от последних можно избавиться при помощи вычитания:

$$\Delta\left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle = \left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle - \left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_{\alpha_1=0} - \left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_{\alpha_2=0} + \left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_{\alpha_1=\alpha_2=0}, \tag{52}$$

где индексы при усреднении означают, что тот или иной ток выключен. Соответственно, в среднем $\left\langle \hat{x}(t_1)\hat{x}(t_2)\right\rangle_{\alpha_1=0}$ содержаться лишь автокорреляции второго тока, как это было посчитано в [26].

В выражении (51) появляется корреляционная функция свободного осциллятора, что означает, что полезный сигнал будет наблюдаться на фоне шума. Как мы увидим в следующем параграфе, от этого недостатка можно избавиться, измеряя координаты нескольких осцилляторов, связанных с изучаемыми электрическими токами.

4.4 Измерение корреляторов для большего количества токов.

Чтобы показать дальнейшее применение развитой техники, рассмотрим случай корреляторов высоких порядков на примере трех токов. Мы оставляем те же предположения относительно электронных времен и временных масштабов, которые будут нас интересовать: $|t_i - t_j| \sim \tau_{el} \gg \gamma^{-1}$.

Сейчас у нас имеется три изучаемых тока, и нам следует производить редукцию матрицы плотности три раза. В этом случае вычисления будут похожи на вычисления предыдущего параграфа, но сейчас мы не сможем применить тот же самый трюк с выделением коммутатора двух операторов координат из под усреднения по матрице плотности, потому что в этом случае мы не сможем посчитать выражение: $\left\langle \left\{\hat{x}(t')\hat{x}(t_1)\right\}\left\{\hat{x}(t'')\hat{x}(t_2)\right\}\right\rangle$ как произведение двух средних от антикоммутаторов. По этой причине рассмотрим эксперимент в котором имеется три различных механических осциллятора, каждый из которых взаимодействует только с одним током. В этом случае гамильтониан взаимодействия имеет вид:

$$\hat{H}_I(t) = \alpha_1\hat{x}_1\hat{I}_1(t) + \alpha_2\hat{x}_2\hat{I}_2(t) + \alpha_3\hat{x}_3\hat{I}_3(t), \tag{53}$$

где $\hat{x}_1$, $\hat{x}_2$ и $\hat{x}_3$ - это операторы координат различных осцилляторов.

Выражение для тройного коррелятора координат может быть получено точно так же, как и в случае двойного коррелятора: (23)-(32). Со старым определением (33) мы получим:

$$\left\langle \hat{x}_1(t_1)\hat{x}_2(t_2)\hat{x}_3(t_3)\right\rangle = \mathrm{Tr}\left[\hat{S}(t_3,t_2)D\Big\{\hat{S}(t_2,t_1)D\big\{\hat{S}(t_1,-\infty)\hat{\rho}(-\infty)\hat{S}^\dagger(t_1,-\infty)\hat{x}(t_1)\big\}_{t_1}\hat{S}^\dagger(t_2,t_1)\hat{x}(t_2)\Big\}_{t_2}\hat{S}^\dagger(t_3,t_2)\hat{x}(t_3)\right], \tag{54}$$

где $t_3 > t_2 > t_1$.

Как и в случае двух токов, мы можем подставить сюда выражения для матрицы плотности и оператора эволюции. Чтобы оставить только существенные члены из всех кубических, мы воспользовались тем, что затухание у осцилляторов большое, и оставили только те члены, в которых ровно по одному интегрированию возле точек t_1, t_2 и t_3. То что остается, получается из первого порядка разложения по константам взаимодействия в операторе эволюции и матрице плотности. Это имеет логичное физическое обоснование - нам следует учесть хотя бы в первом порядке каждый существенный оператор. Таким образом, мы имеем:

$$\begin{aligned}\left\langle \hat{x}_1(t_1)\hat{x}_2(t_2)\hat{x}_3(t_3)\right\rangle = \left\langle \hat{x}_1(t_1)\hat{x}_2(t_2)\hat{x}_3(t_3)\right\rangle_0 + \sum_{k=1}^{3}\sum_{l=1}^{3}\sum_{m=1}^{3}\left(-\tfrac{i}{\hbar}\right)^3\alpha_k\alpha_l\alpha_m \int\limits_{-\infty}^{t_1}dt'\int\limits_{t_1}^{t_2}dt''\int\limits_{t_2}^{t_3}dt'''\left\langle[\hat{x}_m(t''')\hat{x}_m(t_3)]\right\rangle \\ \Big(+\left\langle[\hat{x}_k(t')\hat{x}_k(t_1)]\right\rangle\left\langle[\hat{x}_l(t'')\hat{x}_l(t_2)]\right\rangle\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{S} + \left\langle[\hat{x}_k(t')\hat{x}_k(t_1)]\right\rangle\left\langle\{\hat{x}_l(t'')\hat{x}_l(t_2)\}\right\rangle\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{A_1} \quad (55) \\ +\left\langle\{\hat{x}_k(t')\hat{x}_k(t_1)\}\right\rangle\left\langle\{\hat{x}_l(t'')\hat{x}_l(t_2)\}\right\rangle\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{A_2} + \left\langle\{\hat{x}_k(t')\hat{x}_k(t_1)\}\right\rangle\left\langle[\hat{x}_l(t'')\hat{x}_l(t_2)]\right\rangle\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{A_3}\Big),\end{aligned}$$

здесь мы усредняли все коммутаторы и антикоммутаторы по отдельности, потому что операторы координаты для разных осцилляторов действуют в различных гильбертовых пространствах и коммутируют друг с другом. Обозначения для корреляторов токов имеют следующий вид:

$$\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{S} = \tfrac{1}{4}\left\langle+\hat{I}_m(t''')\hat{I}_l(t'')\hat{I}_k(t')+\hat{I}_k(t')\hat{I}_m(t''')\hat{I}_l(t'')+\hat{I}_l(t'')\hat{I}_m(t''')\hat{I}_k(t')+\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle \quad (56)$$

$$\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{A_1} = \tfrac{1}{4}\left\langle-\hat{I}_m(t''')\hat{I}_l(t'')\hat{I}_k(t')-\hat{I}_k(t')\hat{I}_m(t''')\hat{I}_l(t'')+\hat{I}_l(t'')\hat{I}_m(t''')\hat{I}_k(t')+\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle \quad (57)$$

$$\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{A_2} = \tfrac{1}{4}\left\langle+\hat{I}_m(t''')\hat{I}_l(t'')\hat{I}_k(t')-\hat{I}_k(t')\hat{I}_m(t''')\hat{I}_l(t'')-\hat{I}_l(t'')\hat{I}_m(t''')\hat{I}_k(t')+\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle \quad (58)$$

$$\left\langle\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle^{A_3} = \tfrac{1}{4}\left\langle-\hat{I}_m(t''')\hat{I}_l(t'')\hat{I}_k(t')+\hat{I}_k(t')\hat{I}_m(t''')\hat{I}_l(t'')-\hat{I}_l(t'')\hat{I}_m(t''')\hat{I}_k(t')+\hat{I}_k(t')\hat{I}_l(t'')\hat{I}_m(t''')\right\rangle \quad (59)$$

Окончательный результат получается при интегрировании, имеющем такой же вид, как (49) и (50):

$$\begin{aligned}\left\langle\hat{x}_1(t_1)\hat{x}_2(t_2)\hat{x}_3(t_3)\right\rangle = \sum_{k,l,m}\frac{\alpha_k\alpha_l\alpha_m}{\omega_k^2\omega_l^2\omega_m^2}\Bigg\{\left\langle\hat{I}_k(t_1)\hat{I}_l(t_2)\hat{I}_m(t_3)\right\rangle^{S} - i\left\langle\hat{I}_k(t_1)\hat{I}_l(t_2)\hat{I}_m(t_3)\right\rangle^{A_1}\left(\frac{\gamma_l^2}{\omega_l^2}\frac{2T_l}{\hbar\gamma_l}\right) - \quad (60) \\ -i\left\langle\hat{I}_k(t_1)\hat{I}_l(t_2)\hat{I}_m(t_3)\right\rangle^{A_3}\left(\frac{\gamma_k^2}{\omega_k^2}\frac{2T_k}{\hbar\gamma_k}\right) - \left\langle\hat{I}_k(t_1)\hat{I}_l(t_2)\hat{I}_m(t_3)\right\rangle^{A_2}\left(\frac{\gamma_k^2}{\omega_k^2}\frac{2T_k}{\hbar\gamma_k}\right)\left(\frac{\gamma_l^2}{\omega_l^2}\frac{2T_l}{\hbar\gamma_l}\right)\Bigg\}, \quad (61)\end{aligned}$$

здесь мы ввели обозначения для температур, резонансных частот и коэффициентов затухания для различных осцилляторов, и учли, что для независимых осцилляторов без взаимодействия с резервуарами: $\left\langle\hat{x}_1(t_1)\hat{x}_2(t_2)\hat{x}_3(t_3)\right\rangle_0 = 0$

4.5 Возможная экспериментальная реализация.

Недавние эксперименты с наноэлектро-механическими осцилляторами [23], [24] показывают возможность изучения осцилляторов в вырожденных по температуре квантво-механических состояниях. Рассмотрим в качестве примера механические осцилляторы, которые являются модификацией [24]. В таком приборе осцилляторами являются бруски, закрепленные с двух концов. Пусть каждый из них подключен к большому напряжению, которое позволяет расположенному рядом одноэлектронному транзистору измерять смещение бруска практически с квантовой точностью [Рис.

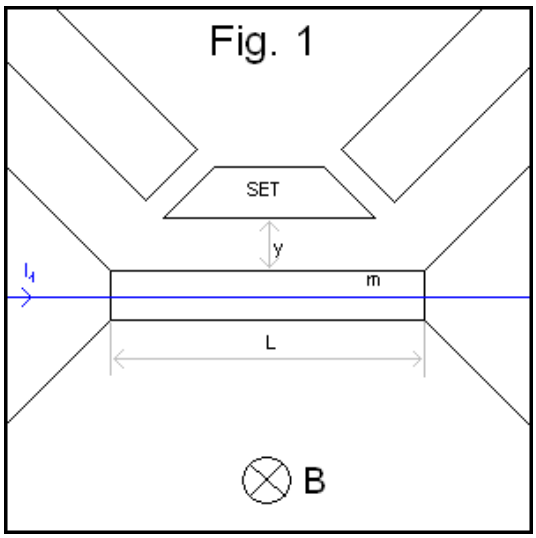

Рис. 1: Экспериментальная установка, использующая одноэлектронный транзистор для измерения смещения наноэлектро-механического осциллятора. Вся система помещена в сильное магнитное поле B. Сила Ампера, действующая на брусок, пропорциональна току I_1, и смешение бруска y прямопропорционально этой силе. Брусок поддерживается при постоянном большом потенциале U, который наводит на островке одноэлектронного транзистора дополнительный заряд, который зависит от расстояния между бруском и островком.

1]. Пусть масса бруска m, его длина l и его собственная резонансная частота ω_0. Предполагается, что каждый из изучаемых токов протекает через один из осцилляторов. Если всю систему поместить в достаточно сильное магнитное поле, то электрические токи, из-за силы ампера, будут раскачивать бруски.

Если ток через брусок порядка I, тогда сила ампера через него будет равна $F_a = IBl$. Так что константа взаимодействия равняется:

$$\alpha = \frac{Bl}{\sqrt{m}}, \tag{62}$$

здесь появилась масса, потому что величина x в формуле (35) равняется реальному смещению y бруска деленному на квадратный корень от массы.

В эксперименте, при помощи нескольких одноэлектронных транзисторов, будет измеряться зависимость смещения x_i каждого бруска от времени. Затем по этим данным считаться корреляционная функция (51) или (61), из которой уже можно извлечь желаемый коррелятор электрических токов.

Заключение

В предложенном способе кодирования информации число сообщений, которое Ева должна перехватить для взлома шифра, экспоненциально по числу кубитов и использованных квантовых вентилей. Это видно из оценок (6), (14) и (19).

Согласно полученным оценкам, Еве необходимо определить структуру всех 2^K запутанных состояний, то есть перехватить

$$N \approx C * 2^{2K} \tag{63}$$

сообщений. Что соответствует передаче

$$N_{bit} \sim K * 2^{2K} \tag{64}$$

битов классической информации.

С другой стороны, согласно (14) Алисе и Бобу необходимо условиться о M натуральных числах, каждое из которых не больше L, чтобы задать последовательность простых унитарных преобразований. Как мы отмечали ранее, M и K должны быть порядка K^2, тем самым, количество информации в битах, необходимой, чтобы описать квантовую сеть вентилей, задается оценкой:

$$N_{key} \sim K^2 * \log_2 K^2. \tag{65}$$

Это выражение определяет длину секретного ключа, которым должны обладать Алиса и Боб. Они могут использовать протоколы генерации секретного ключа использующие квантовую механику. Выражение (64) показывает, сколько классических битов может быть секретно передано, используя этот секретный ключ. Таким образом, предложенная схема шифрования является квантовым аналогом классических схем блочного шифрования.

Хотя предложенный протокол требует наличия заданного секретного ключа, он все еще имеет преимущества перед классическими схемами блочного шифрования, которые тоже считаются защищенными в течение экспоненциального времени по длине секретного ключа. Пример схемы RSA и Шоровского алгоритма факторизации больших чисел показывает, что квантовая механика может значительно упростить взламывание шифров основанных на сложности классических алгоритмов. В противоположность этому, защищенность предложенного протокола определяется фундаментальными законами природы.

Главными преимуществами предложенной схемы является то, что Алиса и Боб однажды договорившись о секретном преобразовании, могут использовать его в течение длительного времени. Передача сообщений происходит в одном направлении, в противоположность протоколам разделения ключа, которые требуют передачу классической информации как от Алисы к Бобу, так и в обратном направлении.

Следует отметить, что согласно главе 2, к классическим проблемам криптографии добавляется проблема определения унитарного преобразования. Источником дополнительной безопасности является теорема о запрете клонирования состояния квантово-механической системы [30]. Согласно этой теореме, измерение квантово-механического состояния в неверном базисе дает меньшее количество информации, чем в классическом случае, где каждое перехваченное сообщение может быть использовано для криптоанализа. В квантовом случае часть перехваченных запутанных состояний необходимо использовать для определения унитарного преобразования.

С другой стороны, согласно теореме о запрете клонирования [30], Ева уничтожает состояние, измеряя его в неправильном базисе, и, тем самым, она не может послать то же самое состояние Бобу. В согласии с основными принципами квантовой криптографии [6], Боб может заметить попытки подслушивания, и он может попросить Алису прекратить передачу сообщений. А так же, по аналогии с релятивистской квантовой криптографией [31], Боб может определить попытки подслушивания по временным задержкам поступающих сообщений.

Хотя рассмотренная схема шифрования имеет преимущества перед остальными, существуют трудности в ее реализации. Во-первых, конструирование квантовых компьютеров, оперирующих десятками кубитов, это все еще дело будущего; даже квантовая томография без использования квантовых компьютеров на данный момент имеет сложности в реализации. Во-вторых, из-за малых времен декогерентности массивных запутанных частиц, фотоны остаются лучшими объектами для передачи квантовых состояний. Но преобразование состояния кубитов в состояние фотонов - это не простая экспериментальная задача. Однако, производятся некоторые попытки по изучению взаимодействия фотонов со сверхпроводниковыми кубитами [27], и изучается возможность преобразования состояния запутанных электронов в запутанное состояние поляризации фотонов [28]. Наконец, в процессе передачи фотонов происходит неизбежное влияние окружающей среды на их состояние, поэтому необходимо применять методы квантовой коррекции ошибок [29].

В заключение, мы предложили оценки, показывающие, что для предложенного криптографического протокола время, в течение которого может быть использовано секретное унитарное преобразование, экспоненциально по числу кубитов в запутанных состояниях, и числу квантовых вентилей, использованных для создания квантового компьютера.

По материалам введения и глав 1, 2 и 3 была написана статья: K.V. Bayandin, G.B. Lesovik, JETP Letters, Vol. 81, No. 7, 2005, pp. 351-355.

Список литературы

[1] R. Feynman, Int. J. Theor. Thys. **21**, 467, (1982)

[2] D. Deutsch, Proc. R. Soc. London A **400**, 97, (1985)

[3] S.I.A.M. Journal on Computing, **26**, 1484, (1997),

[4] R. Rivest, A. Shamir, L. Adleman, *On Digital Signatures and Public Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979)

[5] Dirk Bouwmeester, Artur Ekert, Anton Zeilinger, *The Physics of Quantum Information*, Springer-Verlag (2000)

[6] C. H. Bennet and G. Brassard, *Proc. IEEE Int. Conference on Computer Systems and Signal Processing*, IEEE, New York, (1984)

[7] C. H. Bennet et al, J. Cryptol. **5**, 3 (1992)

[8] A. Muller, J.Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993)

[9] A.K. Ekert, J.G. Rarity, P.R. Tapster, G.M. Palma , Phys. Rev. Lett. **69**, 1293 (1992)

[10] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Hol, Phys. Rev. Lett.**23**, 880 (1969)

[11] G.M D'Ariano, L. Maccone, M. Paini, quant-ph/0210105

[12] W.H. Press, S.A. Teukolsky, W.T. Veterlingt, B.P. Flannery, *The Art of Scientific Computing*, Chapters 7.6 and 7.8, Cambrige University Press (1988-1992)

[13] M. H. Devoret, A. Wallraff, and J. M. Martinis, cond-mat/0411174

[14] *Cavity Quantum Electrodynamics, Advances in atomic, molecular and optical physics*, Supplement 2, P. Berman editor, Academic Press (1994);
S. Haroche, in *Fundamental systems in quantum optics, les Houche summer school session LIII*, J. Dalibard, J.M. Raimond and J. Zinn-Justin eds, North Holland, Amsterdam (1992)

[15] J.I. Cirac and P. Zoller, Phys. rev. Lett. **74**, 4091 (1995);
J.F. Poyatos, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998)

[16] N.A. Gershenfeld and I.L. Chuang, Science **275**, 350 (1997)

[17] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733

[18] G. Lesovik, Th. Martin, G. Blatter, Eur. Phys. J. B **24**, 287, (2001); N. M. Chtchelkatchev, G. Blatter, G. Lesovik, Th. Martin, Phys. Rev. B **66**, 161320, (2002).

[19] C. W. J. Beenakker, C. Emary, M. Kindermann, J. L. van Velsen, Phys. Rev. Lett. **91**, 147901, (2003).

[20] Denis Feinberg, Pascal Simon, App. Phys. Lett. **85**, 1846 (2004).

[21] R. Fiederling et al., Nature (London) **402**, 787 (1999); Y. Ohno et al., ibid., 790 (1999).

[22] C.W.J. Beenakker, C. Emary, M. Kindermann, Phys.Rev.B **69**, 115320 (2004)

[23] A. Robert G. Knobel, Andrew N. Cleland, Nature, **424**, 291 (2003).

[24] M.D. LaHaye, O. Buu, B. Camarota, K.C. Schwab, Science, **304**, 74-77 (2004).

[25] G.B. Lesovik, R. Loosen, JETP Letters **65**, No. 3, 280-284 (1997).

[26] G.B. Lesovik, Usp. Phys. Nauk **168**, No. 2, 155-159 (1998).

[27] A. Wallraff, D.I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S.M. Girvin, and R.J. Schoelkopf, Nature (London) **431**, 162-167 (2004)

[28] V. Cerletti, O. Gywat, D. Loss, cond-mat/0411235

[29] E. Knill, R. Laflamme, Phys. Rev. A **54**, 900-911 (1997)

[30] W.K. Wooters and W.H. Zurek, Nature (London), **299**, 802, (1982)

[31] S.N.Molotkov, S.S.Nazin, quant-ph/0106046