Математические структуры и моделирование 2020. № 2(54). С. 100–128

УДК 550.37 : 550.837
DOI 10.24147/2222-8772.2020.2.100-128

ПРОТОКОЛЫ КВАНТОВОЙ СТЕГАНОГРАФИИ

Д.Э. Вильховский
ассистент, e-mail: vilkhovskiy@gmail.com
А.К. Гуц
д.ф.-м.н., профессор, e-mail: guts@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Цель данной статьи — представить методы современной квантовой стеганографии и сделать небольшой обзор разных типов протоколов квантовой стеганографии.

Ключевые слова: квантовая стеганография, скрытые секретные данные, квантовая связь, запутанные состояния.

1. Введение

Цель данной статьи — представить методы современной квантовой стеганографии и сделать небольшой обзор разных типов протоколов *квантовой стеганографии*.

Стеганография — это техника сокрытия секретной информации в невинно выглядящей информации (например, текст, аудио, изображение, видео и пр.). Стеганосистема — это совокупность средств и методов, которые используются с целью формирования скрытого (незаметного) канала передачи информации.

Скрываемое сообщение (изображение) встраивается в некий не привлекающий внимания объект, называемый *контейнером*, который в результате становится *стегоконтейнером* и затем открыто пересылается адресату.

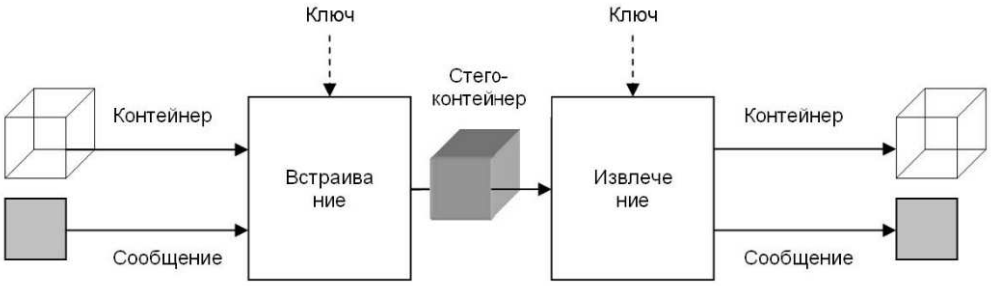

Рис. 1. Обобщённая модель стеганографической системы [1]. Сообщение — данные любого типа, контейнер — любая информация, пригодная для сокрытия в ней сообщений, стегоконтейнер — контейнер, содержащий скрытое сообщение. Стегоконтейнер должен беспрепятственно проходить по каналу связи, никоим образом не привлекая внимания потенциального противника.

Эта статья посвящена обзору протоколов квантовой стеганографии. Данное направление в стеганографии появилось в 1990-е годы и интенсивно развивается в настоящее время.

В стеганографии протоколы, посредством которых передаются секретные сообщения, как и их существование, должны обеспечивать им незаметность, скрытность. Квантовая стеганография использует квантовомеханические эффекты, в том числе квантовой связи и квантовых вычислений, чтобы решить квантовые или классические задачи сокрытия информации. Благодаря теореме о запрете клонирования квантовых состояний[1], а также принципу неопределённости Гейзенберга, согласно которому любая попытка измерить состояние квантовой системы будет нарушать его и поэтому вторжение неизбежно предупреждает законных пользователей о присутствии подслушивающего. Таким образом, квантовая стеганография способствует созданию системы безопасности без подслушивания.

Сокрытие одного квантового состояния в другом основано на трёх основных методах [2, с. 33]:

1) сокрытие в форматах квантовых данных (состояниях), протоколах и т. д.

2) сокрытие с использованием квантовых кодов, исправляющих ошибки;

3) сокрытие в квантовом шуме.

Информация, в том числе и изображения, преобразуются в состояние некоторой квантовой физической системы, т. е. в квантовое состояние, являющееся квантовой информацией, вкладывается в другое квантовое состояние, т. е. в квантовый контейнер. Получаем квантовый стегоконтейнер, который затем передаётся по квантовому каналу связи.

В статье, чтобы явно указать владельца кубита, мы прикрепляем индекс P к каждому состоянию, то есть $|x\rangle_P$ означает, что владелец P имеет состояние $|x\rangle$. Мы используем A и B в качестве индексов, соответствующих Алисе (отправителю секретных сообщений) и Бобу (получателю секретных сообщений) соответственно.

2. Квантовые каналы связи

Квантовые каналы связи, или *квантовая телекоммуникация*, — это способы передачи информации как квантовой, так и классической, посредством аппаратуры, представляющей собой квантовые физические системы, информация в которых передаётся с помощью квантовых объектов. Работа квантовых физических систем описывается с обязательным привлечением принципов квантовой механики.

Таким образом, имеем квантовую информацию ρ на *входе* и квантовую информацию ρ' на *выходе*. Формально квантовый канал — это отображение

[1]Не существует унитарного оператора (гейта) U, осуществляющего преобразование $U|0a\rangle \to |aa\rangle$ для любого a.

$\rho \to \Phi[\rho] = \rho'$, преобразующее квантовое состояние [3]. Например, *деполяризирующий канал* (с вероятностью ошибки p) задаётся формулой

$$\Phi[\rho] = (1-p)\rho + p\frac{1}{d}Tr\rho,$$

где $d = dimH$, H — гильбертово пространство состояний рассматриваемой системы.

В квантовой стеганографии как контейнер, так и секретная информация, и, следовательно, стегоконтейнер, передаваемый по квантовому каналу связи, являются суперпозицией квантовых состояний и рассматриваются как квантовая информация. Поскольку квантовую информацию по теореме о запрете клонирования невозможно размножить, то передача квантовой информации в форме стегоконтейнера по квантовому каналу связи имеет специфику.

Квантовые каналы могут быть привычными физическими устройствами, например, такими как *оптоволоконная линия*, по которой перемещаются поляризованные фотоны, являющиеся квантовыми объектами и переносящими информацию посредством своего квантового состояния, и специфическими, или подобными квантовой телепортации.

Квантовая телепортация — это квантовая двухканальная передача информации о квантовом состоянии системы. Точнее, квантовая телепортация — передача квантового состояния на расстояние при помощи разъединённых и разведённых в пространстве сцепленных (запутанных) входа и выхода канала, а также классического канала связи. При телепортации квантовое состояние разрушается в точке отправления (на входе в канал) при проведении измерения, после чего воссоздаётся в точке приёма (на выходе канала) (рис. 2).

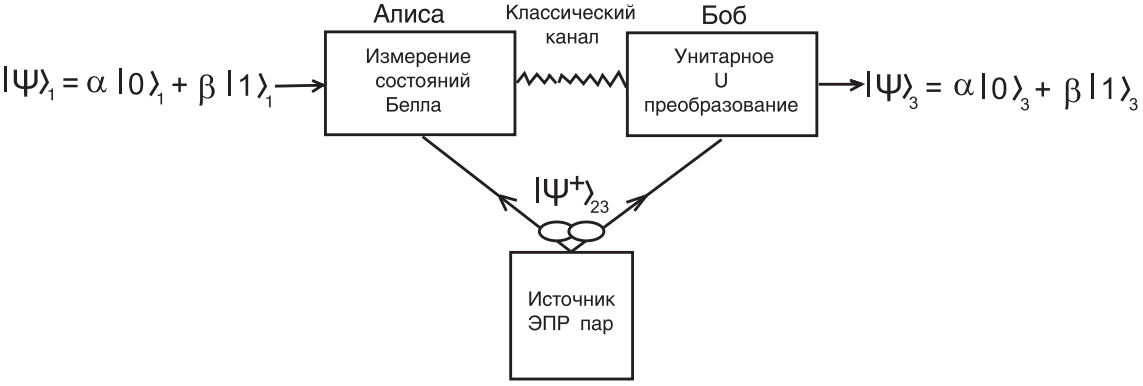

Рис. 2. Схема квантовой телепортации через сцепленную пару (ЭПР-пару). Здесь индексы 1, 2 метят частицы, которыми обладает Алиса, а 3 — Боб. Состояние частицы 1 передаётся частице 3, а сама она теряет исходное состояние и оказывается в сцепленном состоянии с частицей 2 в соответствии с теоремой о запрете клонирования

Важно отметить, что посредством квантовой телепортации передаётся квантовое состояние в форме квантовой суперпозиции

$$\text{Алиса} \ni \sum_i \alpha_i|i\rangle \quad \underset{\text{сцепленные вход и выход}}{\overset{\text{телепортация}}{\longrightarrow}} \quad \sum_i \alpha_i|i\rangle \in \text{Боб}.$$

3. Квантовые протоколы

Для достижения целей в стеганографии имеются протоколы. Под протоколом понимается некоторая последовательность, «порядок действий, предпринимаемых двумя или более сторонами, предназначенный для решения определённой задачи» [4].

Протокол состоит из шагов. На каждом шаге протокола выполняется ряд действий, которые могут заключаться, например, в производстве каких-то вычислений или в осуществлении некоторых действий.

Стеганографические протоколы не шифруют данные, а скрывают место их нахождения в стегоконтейнере. Конечно, спрятанные данные могут быть дополнительно зашифрованы обычными методами, но этот вопрос уже не относится к стеганографии.

Есть четыре типа схем квантовой стеганографии по методам вложения секретной информации:

1) протокол, основанный на классическом I или квантовом изображении $|I\rangle$ (см. § 5);

2) протокол, который использует некоторые физические свойства квантовых состояний для того, чтобы встроить и восстановить секретное сообщение с помощью как локальных квантовых операций, так и классических коммуникаций (§ 6, 7);

3) протокол, который основан на квантовом коде, исправляющем ошибки (§ 8);

4) протокол сокрытия квантовой информации маскированием её под квантовый шум в кодовом слове (§ 9).

4. Алгоритм преобразования классического изображения в квантовое состояние

Основное назначение данного алгоритма — конвертация исходного классического изображения в квантовый вид, т. е. в форму квантовой суперпозиции (квантового состояния, квантовой информации), с целью последующего применения квантовых алгоритмов (например, алгоритма Гровера или квантовых геометрических преобразований). Возможны различные способы конвертации. Представим простейший из них [5].

Представляемый квантовый подход предполагает, что каждый пиксель изображения $x(i, j)$ должен быть преобразован в квантовое состояние

$$|q_{ij}\rangle = c_0|0\rangle + c_1|1\rangle,$$

$c_0, c_1 \in \mathbb{C}$ — амплитуды вероятности того, что после измерения состояние будет 0 и 1 соответственно, причём выполняется следующее условие:

$$|c_0|^2 + |c_1|^2 = 1.$$

Изображение на экране представляется в виде квантовой суперпозиции и создаётся в несколько шагов [5].

Кодирование цветов пикселей, представленных в виде вещественных чисел, в комплексные амплитуды квантовых состояний, осуществляется с помощью функции

$$\delta : \mathbb{R}^3 \to \mathbb{C}^3, \quad \delta : (x_1, x_2, x_3) \to (r_1 e^{i\phi_1}, r_2 e^{i\phi_2}),$$

где x_1, x_2, x_3 — компоненты цветовой модели RGB (red, green, blue), $r_1 = \sqrt{1 - x_3^2}$, $r_2 = x_3$, $\phi_1 = \arcsin(2x_1 - 1)$, $\phi_2 = \arcsin(2x_2 - 1)$.

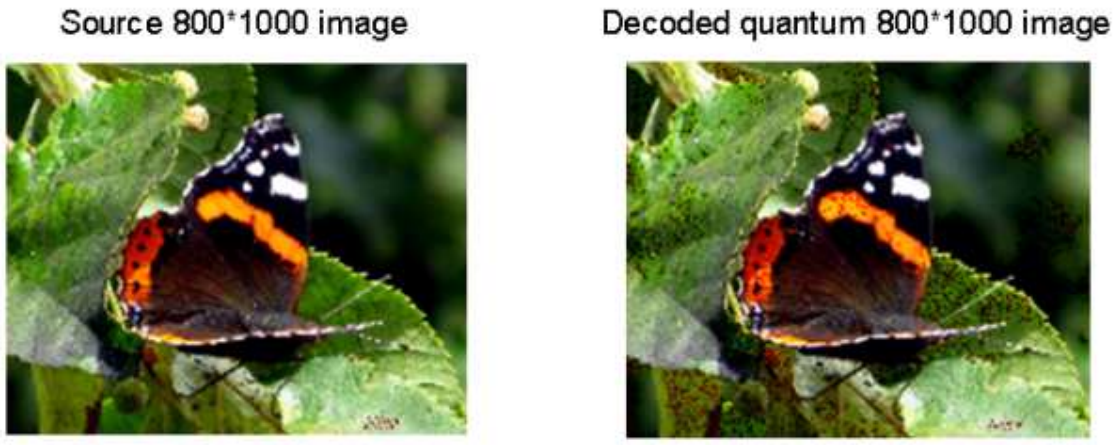

Рис. 3. Декодирование исходного изображения из квантовой суперпозиции. Количество неправильно декодированных пикселей: 64973 из 800000 (8.1%) [5]

Пусть $c_1 = r_1 e^{i\phi_1}, c_2 = r_2 e^{i\phi_2}$, тогда имеем цвет пикселя в x_k $(k = 0, .., 2^{2n-1})$ виде:

$$|q_k\rangle = c_1|0\rangle + c_2|1\rangle.$$

Обратное преобразование выполняется по следующей схеме:

$$\delta^{-1} : \mathbb{C}^3 \to \mathbb{R}^3, \quad \delta^{-1} : (c_1, c_2) \to \left(\frac{1 + \phi_1}{2}, \frac{1 + \phi_2}{2}, |c_2| \right).$$

Кодирование координат k-го пикселя осуществляется следующим образом:

$$|k\rangle = |x_{n-1}...x_0\rangle \otimes |y_{n-1}...y_0\rangle,$$

где состояния $|x\rangle$ и $|y\rangle$ кодируют координаты пикселей (номера столбца и строки пикселя соответственно).

В результате изображение I представляется квантовой суперпозицией квантовых пикселей

$$|I\rangle = \frac{1}{2^n} \sum_{k=0}^{2^{2n-1}} |q_k\rangle \otimes |k\rangle.$$

Таким образом, изложенный алгоритм представляет изображение, состоящее из множества пикселей, в виде единой суперпозиции, содержащей характеристики всех пикселей изображения (но так как в данном случае идёт речь о модели квантового алгоритма и хранении пикселей на классическом компьютере, то амплитуды вероятности и вектора состояния, являющиеся слагаемыми суперпозиции, хранятся как отдельные значения).

Восстановление исходного изображения из квантовой суперпозиции носит более сложный характер. Результаты декодирования классического изображения из квантового состояния суперпозиции представлены на рис. 1.

5. Вложение в изображение. Протокол, основанный на QUALPI-модели

Данный протокол (2019, [6]) может не только обеспечивать хорошую незаметность и безопасность, но и большую полезную нагрузку для скрываемой информации благодаря неплохой масштабируемости кодирования информации.

5.1. Подготовка квантового изображения в QUALPI-модели

В 2013 году Zhang Yi и др. [7] предложили QUALPI-модель представления на основе log-полярных координат классического изображения I в форме квантовой суперпозиции $|I\rangle$ с целью его хранения и обработки.

Квантовое log*-полярное изображение* (QUALPI) с разрешением $2^m \times 2^n$ и с разрешением уровня серого 2^q все пиксели задаёт как квантовую суперпозицию вида:

$$|I\rangle = \frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} |g(\rho,\ \theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle, \tag{5.1}$$

$$g(\rho,\ \theta) = C_0 C_1 \cdots C_{q-2} C_{q-1}, \quad g(\rho,\ \theta) \in [0, 2^q - 1]. \tag{5.2}$$

Здесь ρ — логарифм расстояния, представляет информацию о пикселе изображения в радиальном направлении, а θ — полярный угол. Пара (ρ, θ) представляет позицию пикселя изображения, $g(\rho, \theta)$ даёт серое значение пикселя. Процесс подготовки квантовых изображений подробно изложен в [7].

Определяется операция вращения квантовых QUALPI-изображений. Угол поворота задаётся в форме его бинарного кода (регистра):

$$R_x = r_0 r_1 \cdots r_{n-2} r_{n-1}, \quad r_i \in \{0, 1\}, \quad R_x \in [0, 2^n - 1]. \tag{5.3}$$

Если угол вращения есть R_x, то квантовое изображение будет повёрнуто и сложено n раз. Выполняется 2^k единичных вращений QUALPI-квантового изображения в виде R_{2^k}. Операция определяется следующим образом:

$$R_{2^k}|I\rangle = R_{2^k}\left(\frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} (|g(\rho,\ \theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle)\right) =$$

$$= \frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} \left(|g(\rho,\theta)\rangle \otimes |\rho\rangle \otimes |(\theta + 2^k) \mod 2^n\rangle \right) =$$

$$= \frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} (|g(\rho,\ \theta)\rangle \otimes |\rho\rangle \otimes |(\theta_0\theta_1 \cdot \theta_{n-k-1} + 1) \mathrm{mod}\ 2^{n-k}\rangle) \otimes$$

$$\otimes |\theta_{n-k}\theta_{n-k+1}...\theta_{n-1}\rangle. \qquad (5.4)$$

5.2. Расширение квантового изображения

Квантовое расширение изображения — это расширение изображения до *атласа изображений*, в котором каждое изображение является исходным изображением, повёрнутым на некоторый угол.

Процесс расширения квантового изображения должен выполнить n итераций расширения квантового изображения. Для квантового изображения (5.1) с разрешением $2^m \times 2^n$ и уровнем серого 2^q после n итераций квантовое состояние всей системы будет преобразовано в следующее состояние:

$$|I_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle R_i |I\rangle =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \otimes \left(\frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} |g(\rho,\ \theta)\rangle \otimes |\rho\rangle \otimes |(\theta + i) \mathrm{mod}\ 2^n\rangle \right). \qquad (5.5)$$

Основная операция заключается в повороте соответствующего исходного состояния изображения на 2^{n-1-i} единиц против часовой стрелки, когда i-й квантовый бит двоичного регистра порядкового номера равен $|1\rangle$. Алгоритм подробно описан в [7].

5.3. Схема квантового QUALPI-протокола

Предлагаемый стеганографический протокол использует QUALPI-модель квантового изображения, квантовое расширение изображения и алгоритм поиска Гровера. Он состоит из процессов встраивания и извлечения секретной информации. Блок-схема протокола показана как рис. 2.

5.4. Вложение контейнера с секретной информацией

Контейнер — любая информация, пригодная для сокрытия в ней сообщений. Опишем процесс внедрения секретной информации в квантовый контейнер изображения.

Различные квантовые изображения получаем вращением на разные углы по формуле (5.4). Затем используется алгоритм расширения квантового изображения.

После расширения несущего изображения как наложенного набора изображений секретную информацию можно спрятать в одну из копий изображения

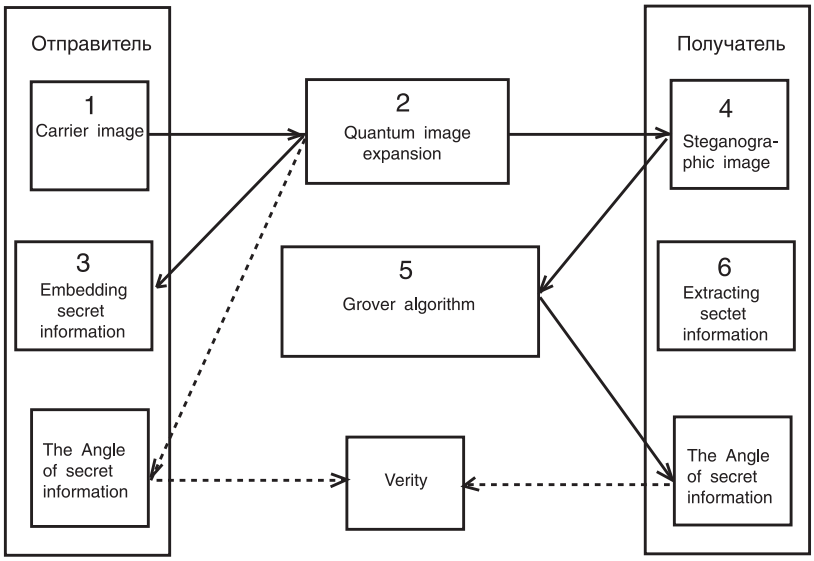

Рис. 4. Схема QUALPI-протокола [6]

с определённым угол поворота θ_1. Согласно правилу кодирования секретная информация может быть представлена углом поворота s, точнее, его двоичным кодом, известным и для Алисы, и для Боба. Так что **процесс встраивания секретной информации — это поворот изображения носителя на угол** $\theta_1 + s$.

Результирующее квантовое состояние после этого процесса даётся следующей формулой:

$$|I_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle R_i |I\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0, i\neq s}^{2^n-1} |i\rangle \otimes \left(\frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} (|g(\rho,\ \theta)\rangle \otimes |\rho\rangle \otimes \right.$$

$$\left. \otimes |(\theta + i) \mathrm{mod}\ 2^n\rangle \otimes (\theta + \theta_1 + s) \mathrm{mod}\ 2^n) \right).$$

5.5. Имитационные эксперименты

Протоколы оцениваются по трём показателям: незаметность, безопасность и вместимость. Незаметность означает, что секретная информация кодируется некоторым углом, а затем встраивается в любое расширенное изображение контейнера (носителя). Это обеспечивает безопасность секретной информации в процессе секретности передачи информации и безопасность секретной информации в канале. Вместимость означает, что в процессе вложения секретной информации секретная информация может быть закодированы углом поворота, а затем встроена в прямом или обратным направлениях поворота несущего изображения.

Возьмём известное изображение Лена.bmp. Размер несущего изображения составляет $2^7 \times 2^8$.

На рис. 3 показаны повёрнутые изображения Лены на 90 градусов, 45 градусов и 1,40625 градуса. Носитель изображения с углом расширения 0 градусов.

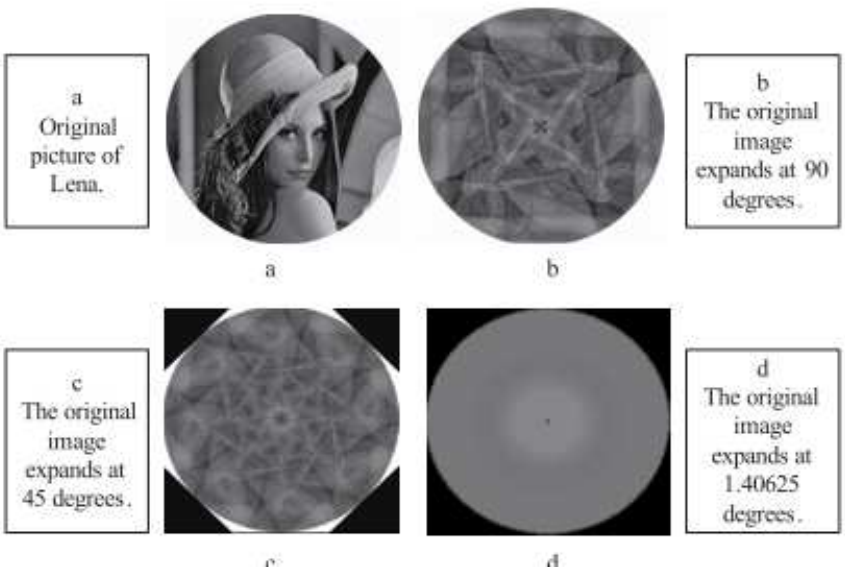

Рис. 5. Повёрнутые изображения Лены [6]

Рис. 6. a) оригинальное изображение Лены: b) Лена, повёрнутая на секретный угол 5°; c) расширенное изображение с загруженной секретной информацией [6]

5.6. Извлечение информации

Процесс извлечения скрытой информации состоит в вычислении угла θ_1 и осуществляется следующим образом.

Шаг 1. Использование алгоритма Гровера для выполнения квантового поиска изображения, чтобы найти то же изображение, что и исходное.

Рассматриваем

$$|I_n\rangle \otimes |-\rangle = \frac{1}{\sqrt{2}} \sum_{i=0}^{2^n-1} |i\rangle R_i|I\rangle \otimes |-\rangle,$$

где

$$|-\rangle = \frac{1}{2}(|0\rangle - |1\rangle).$$

Затем создадим чёрный ящик Oracle U_f и применим чёрный ящик к квантовому состоянию системы. Значение $f(R_i)|I\rangle$, если измеренное изображение $|I'\rangle$ совпадает с исходным изображением, равно 1, иначе это 0. Реализацию функции см. в [50].

$$U_f(|i\rangle R_i|I\rangle|j\rangle) = |i\rangle R_i|I\rangle j \oplus f(R_i),$$

$$f(R_i)|I\rangle = \begin{cases} 1, & \text{если } sim(R_i|I\rangle, |I'\rangle) \ = 1, \\ 0, & \text{иначе.} \end{cases}$$

Функция $f(R_i)|I\rangle)$ устанавливает подобие (сходство) между расширенным изображением $R_i|I'\rangle$ и измеренным изображением $|I'\rangle$. Эволюция всей системы после прохождения чёрного ящика U_f отображается следующим образом:

$$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle R_i|I\rangle \to \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(R_i|I\rangle)} |i\rangle R_i|I\rangle \otimes |-\rangle.$$

Согласно алгоритму поиска Гровера квантовое состояние после завершения $[\frac{\pi}{4}\sqrt{2^n}]$ итерации задаётся следующим образом:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{i=0, i\neq j}^{2^n-1} |i\rangle R_i|I\rangle + (-1)|j\rangle R_j|I\rangle \right),$$

$$|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right) \left(\frac{1}{\sqrt{2^n-1}} \sum_{i=0, i\neq j}^{2^n-1} |i\rangle R_i|I\rangle \right) + \sin\left(\frac{2k+1}{2}\theta\right) |j\rangle R_j|I\rangle.$$

Здесь j — это серийный номер того же изображения, что и исходное изображение в атласе, и $\theta = 2\arccos\sqrt{1-\frac{1}{2^n}}$.

Шаг 2. Производим измерение для извлечения классической секретной информация из $|\psi\rangle$. Если серийный номер j вкладывается как секретная информация, угол поворота секретной информации будет θ_1:

$$|\psi\rangle \to |j\rangle R_j|I\rangle$$

с вероятностью

$$\left|\sin\left(\frac{2k+1}{2}\theta_1\right)\right|^2.$$

6. Вложение в обычный текст. Протокол Михары, использующий ВПР-пары

В этом параграфе рассмотрим протокол квантовой стеганографии, встраивающий секретные сообщения в обычный текст. В целом стеганография встраивания секретных сообщений в обычный текст является более сложной, чем, скажем, встраивание в изображения или в аудиоданные, поскольку мы считаем, что простой текст может сразу показаться подозрительным, даже если внесённые в него изменения были незначительными.

Протокол Михары (2012, [8]), излагаемый ниже, встраивает любой секретный текст без изменения содержания контейнера, состоящего из несекретного текста.

Мы можем использовать несекретный естественный простой текст в качестве сопроводительных данных, используемых в нашем протоколе стеганографии. Поэтому любой перехватчик не может решить, является ли сообщение стегоданными или нет.

Протокол Михары заранее разделят запутанные состояния между Алисой и Бобом в качестве квантовых ключей, используемых, когда стороны восстанавливают секретные сообщения из стегоконтейнера. При этом ни состояния невинной информации, ни секретной информации не включаются в эти запутанные состояния.

Задача состоит в том, чтобы построить такой протокол. Стороны не могут восстановить секретную информацию, используя только локальные квантовые операции, они дополняются классическим общением между ними, хотя этот протокол также делится информацией между ними.

В этом параграфе мы рассматриваем протокол квантовой стеганографии с использованием простого текста в качестве контейнера.

Во-первых, мы создаём квантовое запутанное состояние, представляющее классическое сообщение. Это квантовое состояние и есть контейнер.

Во-вторых, мы создаём квантовый стегоконтейнер, включающий в себя встроенное секретное сообщение, объединённое с квантовым контейнером, содержащим обычный несекретный текст.

6.1. Контейнер

Мы рассматриваем ситуацию, в которой Алиса хочет отправить Бобу классическое сообщение $a \in \{0, 1, ..., N-1\}$ $(N \geqslant 2)$. Это сообщение не является секретным, информация может быть украдена Евой, или Алиса может открыть его намеренно.

В этой ситуации мы строим протокол следующим образом. Во-первых, Алиса создаёт квантовое состояние

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle \otimes |x+r\rangle, \tag{6.1}$$

соответствующее классическому сообщению a, где

— $a \in \{0,1,...,N-1\}$ — случайное число, выбранное Алисой;

— $|\bullet\rangle$ — называем ниже (в § 6) регистром.

Далее везде $|x+r\rangle = |(x+r) \mod N\rangle$.

Алиса может посылать контейнер (6.1) Бобу.

Боб читает полученное сообщение a в форме (6.1), применяя, во-первых, преобразование Фурье

$$|x\rangle \to \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{i2\pi xy/N}|y\rangle$$

к двум регистрам. Именно:

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle \otimes |x+r\rangle \to$$

$$\to \frac{1}{\sqrt{N^3}}\sum_{x=0x}^{N-1N}\sum_{1^{=0}}^{-1}\sum_{x_2=0}^{N-1} e^{-i2\pi ax/N}e^{i2\pi x x_{1/N}}e^{i2\pi(x+r)x_2/N}|x_1\rangle \otimes |x_2\rangle =$$

$$= \frac{1}{\sqrt{N^3}}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1} e^{i2\pi r x_2/N}\Big(\sum_{x=0}^{N-1} e^{i2\pi(x_1+x_2-a)x/N}\Big)|x_1\rangle \otimes |x_2\rangle =$$

$$= \frac{1}{\sqrt{N}}\sum_{x_1+x_2\equiv a(\mathrm{mod}N)} e^{i2\pi r x_{2/N}}|x_1\rangle \otimes |x_2\rangle, \tag{6.2}$$

где использовано свойство, что $\sum_{x=0}^{N-1} e^{i2\pi yx/N} = N$, если $y \equiv 0(\mathrm{mod}\ N)$, и сумма равна нулю, если $y \not\equiv 0(\mathrm{mod}\ N)$.

Во-вторых, Боб может, проводя измерения (6.2) двух регистров, получить x_1 и x_2. Складывая $x_1 + x_2 \equiv a(\mathrm{mod}\ N)$, как видим, он получаем сообщение a.

6.2. Протокол Михары

Обычно стегоконтейнер строится модификацией контейнера, т. е. стегоконтейнер получается вложением секретного сообщения в контейнер. Однако стегоконтейнер в протоколе Михары строится комбинированием двух квантовых состояний, одно из которых — с секретным сообщением s, а второе — с классическим сообщением a, являющимся контейнером. Контейнер имеет вид

$$(1/\sqrt{N})\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle \otimes |x+r\rangle,$$

соответствует сообщению a, и наш стегоконтейнер не строится вложением секретного сообщения s в указанное состояние, а включает квантовое состояние контейнера.

Протокол состоит из следующих шагов.

Шаг 1. Алиса и Боб располагают переплетённым состоянием

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle_A\otimes|y\rangle_B, \tag{6.3}$$

где 1-й регистр принадлежит Алисе, второй — Бобу.

Состояние должно быть надёжно разделённым между сторонами. Обратите внимание, что этот шаг есть установление квантового канала связи между Алисой и Бобом.

Шаг 2. Имея секретное сообщения s, отправляемое Бобу, и сообщение a контейнера, Алиса создаёт состояние

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}|x\rangle,$$

соответствующее сообщению a в контейнере, и встраивает сообщение s в состояние (6.1) на шаге 1 следующим образом:

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}{}^{-i2\pi sy/N}|y\rangle_A\otimes|y\rangle_B.$$

Шаг 3. Алиса объединяет два состояния в Шаге 2 и создаёт запутанное состояние из них, т. е. она добавляет первый регистр ко второму регистру.

$$\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}|x\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{=0}^{N-1}e^{-i2\pi sy/N}|y\rangle_A\otimes|y\rangle_B\right)\to$$

$$\to\frac{1}{\sqrt{N^2}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}e^{-i2\pi ax/N}e^{-i2\pi sy/N}|x\rangle\otimes|x+y\rangle_A\otimes|y\rangle_B=$$

$$=\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{-i2\pi sy/N}\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}|x\rangle\otimes|x+y\rangle_A\right)\otimes|y\rangle_B.$$

Это состояние является стегоконтейнером, соответствующим сообщению s, вложенному в сообщение a.

Обратите внимание, что сообщение s и сообщение a входят в стегоконтейнер без какой-либо связи друг с другом. Поэтому Алиса может использовать любой естественный простой текст a как классический контейнер построения стегоконтейнера, и не нужно изменять это сообщение при построении соответствующего стегоконтейнера.

Шаг 4. Алиса отправляет свои два регистра Бобу. Регистры могут быть открытыми для всех.

Шаг 5. Боб может восстановить секретное сообщение s, применив квантовое преобразование Фурье для всех регистров:

$$\frac{1}{\sqrt{N^2}}\sum_{y=0}^{N-1}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}e^{-i2\pi sy/N}|x\rangle\otimes|x+y\rangle\otimes|y\rangle\to$$

$$\to\frac{1}{\sqrt{N^5}}\sum_{y=0}^{N-1}\sum_{x=0}^{N-1}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_1=0}^{N-1} e^{-i2\pi ax/N}e^{-i2\pi sy/N}\times$$

$$\times e^{i2\pi xx_1/N}e^{i2\pi(x+y)x_2/N}e^{i2\pi yy_1/N}|x_1\rangle\otimes|x_2\rangle\otimes|_1\rangle=$$

$$=\frac{1}{\sqrt{N^5}}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{_1=0}^{N-1}\left(\sum_{x=0}^{N-1}e^{i2\pi(x_1+x_2-a)x/N}\right)\left(\sum_{y=0}^{N-1}e^{i2\pi(_1+x_2-s)y/N}\right)|x_1\rangle\otimes|x_2\rangle\otimes|y_1\rangle=$$

$$=\frac{1}{\sqrt{N}}\sum_{\substack{x_1+x_2\equiv a(mod\ N)\\ y_1+x_2\equiv s(\mod N)}}|x_1\rangle\otimes|x_2\rangle\otimes|y_1\rangle.$$

Затем Боб может восстановить сообщение s, потому что он может получить y_1 и x_2, удовлетворяющие $y_1+x_2\equiv s(\mod N)$, путём измерения состояния (очевидно, он также может восстановить сообщение a).

6.3. Секретность и безопасность

Изучим отношение между данными стегоконтейнера и данными контейнера. Стегоконтейнер на Шаге 3 имеет вид

$$\frac{1}{\sqrt{N^2}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} e^{-i2\pi ax/N}e^{-i2\pi sy/N}|x\rangle\otimes|x+y\rangle\otimes|y\rangle=$$

$$=\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{-i2\pi sy/N}\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}|x\rangle\otimes|x+y\rangle\right)\otimes|y\rangle,$$

а контейнер —

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}|x\rangle\otimes|x+r\rangle.$$

Таким образом, разница между регистрами Алисы, показанными на шаге 4, и данными контейнера не может быть найдена — и то и другое одинаковой формы экспоненты.

Более того, в этом случае любой подслушиватель Ева не сможет отличить данные контейнера от стегоданных, даже если регистры Алисы на шаге 4 раскрыты. Действительно, при измерениях, производимых Евой, секретное данное s и несекоетное a войдут в вероятности замеров регистров:

$$|e^{-i2\pi sy/N}|=|e^{-i2\pi ay/N}|=1.$$

Следовательно, секретность сохраняется.

Далее, даже если Ева применит преобразование Фурье к части стего-контейнера (открытые Алисой):

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi\alpha/N}|x\rangle \otimes |x+y\rangle$$

и измерит два регистра, сообщение s может быть восстановлено Бобом, если он может знать результат, измеренный третьей стороной. Здесь мы наблюдаем ситуацию, при которой Боб выполняет свою процедуру, используя данные контейнера, открытые Алисой, и измеряя их.

Действительно, во-первых, при применении квантового преобразования Фурье, состояние стегоданных становится следующим:

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{-i2\pi my/N}(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle \otimes |x+y\rangle) \otimes |y\rangle \rightarrow$$

$$\rightarrow \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{i2\pi(x_2-m)y/N}\left(\frac{1}{\sqrt{N}}\sum_{x_1+x_2\equiv a(\mathrm{mod}\ N)} |x_1\rangle \otimes |x_2\rangle\right) \otimes |y\rangle.$$

Измерение первых двух регистров даёт только x_1 и x_2, удовлетворяющие $x_1 + x_2 \equiv a(\mod N)$, и, значит, вычисляется только несекретное сообщение a из контейнера.

После описанного измерения, проведённого Евой, квантовое состояние имеет вид

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{i2\pi(x_2-m)y/N}|y\rangle.$$

Поэтому, применяя квантовое преобразование Фурье к его регистру, Боб может получить y_1, удовлетворяющее $y_1 + x_2 \equiv s(\mod N)$.

Кроме того, даже если какая-либо другая операция применяется Евой к стегоконтейнеру, она может воздействовать только на состояние

$$\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle \otimes |x+y\rangle,$$

сцепленное с (каждым) регистром Боба $|y\rangle$. Затем Боб может восстановить секретное сообщение s, поскольку оно относится к регистру Боба. Скрытность секретного сообщения сохраняется.

7. Протокол AMH, использующий сцепленность четырех частиц

Изложим протокол AMH, который предложили A. El Allati, M.B. Ould Medeni и Y. Hassouni (2012, [10]). Его усовершенствовали Shu-Jiang, Chen Xiu-Bo, Niu Xin-Xin и Yang Yi-Xian (2013, [11]). Протокол основан на передаче сообщений с помощью сцепленных четырёх частиц.

7.1. GHZ_4-состояние

Протокол АМН предполагает, что Боб готовит сцепленное состояние Гринбергера–Хорна–Зейлингера из четырёх частиц:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|0000\rangle_{1234} + |1111\rangle_{1234}\Big), \tag{7.1}$$

называемое GHZ_4-состоянием, причём себе оставляет первую и третью частицы P_1, P_3, а вторую и четвертую — P_2, P_4 — отсылает Алисе.

Рассматриваем четыре унитарных преобразования Паули $\sigma_I, \sigma_x, \sigma_y$ и σ_z:

$$\sigma_{\mathrm{I}} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

$$\sigma_y = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}.$$

Применением одного из четырёх приведённых локальных унитарных преобразований к квантовому состоянию частицы её квантовое состояние может быть изменено на другое. Собственные состояния операторов Паули образуют две разные группы ортонормированных базисов $X = \{|x_+\rangle, |x_-\rangle\}$ и $Y = \{|y_+\rangle, |y_-\rangle\}$ в одночастичном пространстве:

$$|x_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{7.2}$$

$$|y_+\rangle = \frac{1}{\sqrt{2}}(|0\} + i|1\rangle), \ |y_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle). \tag{7.3}$$

Используя эти две группы базисов, сцепленное GHZ_4-состояние (7.1) можно переписать в четырёх видах:

$$\begin{aligned} |\Psi\rangle = \frac{1}{2\sqrt{2}}[(|x_+\rangle_1|x_+\rangle_2 + |x_-\rangle_1|x_-\rangle_2)(|x_+\rangle_3|x_+\rangle_4 + \\ +|x_-\rangle_3|x_-\rangle_4) + (|x_+\rangle_1|x_-\rangle_2 + |x_-\rangle_1|x_+\rangle_2)\times \\ \times(|x_+\rangle_3|x_-\rangle_4 + |x_-\rangle_3|x_+\rangle_4)] = |\Psi_1\rangle, \end{aligned} \tag{7.4}$$

$$\begin{aligned} |\Psi\rangle = \frac{1}{2\sqrt{2}}[(|y_+\rangle_1|y_+\rangle_2 + |y_-\rangle_1|y_-\rangle_2)(|y_+\rangle_3|y_+\rangle_4 + \\ +|y_-\rangle_3|y_-\rangle_4) + (|y_-\rangle_1|y_-\rangle_2 + |y_-\rangle_1|y_+\rangle_2)\times \end{aligned}$$

$$\times(|y+\rangle_3|y_-\rangle_4 + |y_-\rangle_3|y+\rangle_4)] = |\Psi_2\rangle, \tag{7.5}$$

$$|\Psi\rangle = \frac{1}{2\sqrt{2}}[(|x_+\rangle_1|y+\rangle_2 + |x_-\rangle_1|y_-\rangle_2)(|x_+\rangle_3|y_-\rangle_4 + |x_-\rangle_3|y_+\rangle_4) + (|x_+\rangle_1|y_-\rangle_2 + |x_-\rangle_1|y_+\rangle_2)\times \times(|x_+\rangle_3|y_+\rangle_4 + |x_-\rangle_3|y_-\rangle_4)] = |\Psi_3\rangle, \tag{7.6}$$

$$|\Psi\rangle = \frac{1}{2\sqrt{2}}[(|y_+\rangle_1|x_+\rangle_2 + |y_-\rangle_1|x_-\rangle_2)(|y_+\rangle_3|x_-\rangle_4 + |y_-\rangle_3|x_+\rangle_4) + (|y_+\rangle_1|x_-\rangle_2 + |y_-\rangle_1|x_+\rangle_2)\times \times(|y_+\rangle_3|x_+\rangle_4 + |y_-\rangle_3|x_-\rangle_4)] = |\Psi_4\rangle. \tag{7.7}$$

Вышеуказанные разложения демонстрируют корреляцию между четырьмя частицами. Согласно (7.4)–(7.7), можно кодировать 2^4 различных кодовых слов, используя четырёхбитовые кодовые слова. Например, закодировать состояние $|x_+\rangle_1|x_+\rangle_2|x_+\rangle_3|x_+\rangle_4$ как 0000, тогда в конце можно получить 32 кодовых слова.

Алиса и Боб договариваются о кодовых словах состояний прежде, чем они начнут распределять частицы GHZ_4-состояния.

Также, применяя унитарные преобразования $\sigma_{\rm I}\sigma_{\rm I}$, $\sigma_x\sigma_x$, $\sigma_{\rm I}\sigma_z$, $\sigma_y\sigma_y$, $\sigma_{\rm I}\sigma_x$, $\sigma_x\sigma_y$, $\sigma_{\rm I}\sigma_y$ или $\sigma_y\sigma_x$ к второй и четвёртой частицам в $|\Psi_i\rangle(i = 1, 2, 3, 4)$, можно закодировать 3-битовые секретные сообщения, используя правила кодирования, данные в табл.1.

Таблица 1. Корреляция между преобразованиями и всевозможными кодами

Унитарное преобразование Алисы	Код	Унитарное преобразование Алисы	Код
$U_1 = \sigma_I\sigma_I$	000	$U_5 = \sigma_x\sigma_x$	100
$U_2 = \sigma_I\sigma_z$	001	$U_6 = \sigma_y\sigma_y$	101
$U_3 = \sigma_I\sigma_x$	010	$U_7 = \sigma_x\sigma_y$	110
$U_4 = \sigma_I\sigma_y$	011	$U_8 = \sigma_y\sigma_x$	111

7.2. Протокол AMH

Протокол AMH состоит из следующих шагов.

Боб посылает квантовый регистр из n состояний $|\Psi\rangle^{\otimes n} = |\Psi\rangle_1|\Psi\rangle_2 \ldots |\Psi\rangle_n$, в котором находится контейнер сообщения для получателя. Позже Алиса случайным образом выбирает достаточно большое подмножество частиц из регистра в качестве проверочной группы $\{P_{1,ch}, P_{2,ch}, P_{3,ch}, P_{4,ch}\}$ для проверки безопасности квантового канала. По классическому каналу Алиса сообщает Бобу выбранные частицы. Обратите внимание, что каждая проверяемая частица измеряется случайным образом в одном из четырёх состояний $|x_+\rangle, |x_-\rangle, |y_+\rangle, |y_-\rangle$,

как в протоколе BB84. А также другие частицы $\{P_{1,c}, P_{2,c}, P_{3,c}, P_{4,c}\}$, которые называются группой коммуникации, сообщением контейнера. Затем Алиса выбирает случайным образом между состояниями связи, чтобы скрыть секретное сообщение, используя унитарные преобразования U_i для обеих частиц P_2 и P_4. Детали алгоритма схемы выглядят следующим образом.

Шаг 1. Боб готовит квантовый регистр из n состояний $|\Psi\rangle^{\otimes n} = |\Psi\rangle_1|\Psi\rangle_2 \ldots |\Psi\rangle_n$ и отправляет половину каждого состояния Алисе в виде частиц P_2 и P_4.

Шаг 2. После того, как Алиса получила эти частицы, она проверяет безопасность квантового канала, выбирая случайным образом подмножество состояний, формируя проверочную группу.

Шаг 3. Алиса измеряет эти частицы на основе $X = \{|x_+\rangle, |x_-\rangle\}$ или $Y = \{|y_+\rangle, |y_-\rangle\}$, взятые из контрольной группы, и объявляет их базы измерения и соответствующие результаты измерения по классическому каналу.

Шаг 4. После получения результатов Алисы Боб измеряет свои частицы P_2, P_4 на той же базе измерений и сравнивает свои результаты с результатами Алисы, чтобы обнаружить подслушивание. Если квантовый канал не является безопасным, они останавливают общение и распределяют другой регистр частиц $\{P_{1,n}, P_{2,n}, P_{3,n}, P_{4,n}\}$, в противном случае начинается передача информации.

Шаг 5. Если квантовый канал защищён, Алиса выбирает произвольно много кубитов из группы коммуникации для встраивания скрытого сообщения. Она использует унитарное преобразование, как указано в таблице 1, для частиц P_2 и P_4 соответственно, без измерения частицы как плотный код [12]. Например, Алиса выбирает позиции m, $m+4$, ..., $m+t$ как $|\Psi'\rangle_m, |\Psi'\rangle_{m+4}, ..., |\Psi'\rangle_{m+t}$, и затем она отправляет их Бобу.

Шаг 6. Боб измеряет частицы P_1 и P_3 на основе (7.4)–(7.7) и выполняет измерение путешествующих частиц, что ему послала Алиса. Опираясь на результаты измерения, Боб может различить унитарные преобразования U_i, используемые Алисой, и извлечь скрытое сообщение, используя таблицу 1.

8. Протокол квантовой стеганографии, основанный на квантовом коде, исправляющем ошибки

Цель параграфа — ознакомиться с протоколом, основанным на квантовом коде, исправляющем ошибки (2015, [9]). Причём этот протокол квантовой стеганографию *использует* заранее сцепленные (запутанные) состояния, поступающие в распоряжении Алисы и Боба, для тайной отправки сообщений.

Протокол встраивает секретное сообщение в квантовый код, исправляющий ошибки. Конечно, это влияет на его содержимое, поскольку оно встроено как часть передаваемого кода. Поэтому ошибки, возникающие при передаче, могут привести к повреждению секретного сообщения, если встроенная часть повреждена. Однако, как показывается, ошибки в сопроводительных сообщениях не влияют на содержание секретных сообщений в предлагаемом протоколе.

Сначала мы опишем некоторые основные обозначения. Пусть $\mathrm{B} = \{0, 1\}$. Для бита $b \in \mathrm{B}$ пусть $\bar{b}(= b \oplus 1)$ будет отрицанием b. Для $x_i \in \mathrm{B}$ $(i = 1, 2, \ldots, n)$ мы обозначаем n-битную строку $x \in \mathrm{B}^n$ (т. е. $|x| = n$) через $x = x_1 x_2 \ldots x_n$.

Пусть $x \cdot y = \sum_{i=1}^{\mathrm{n}} x_i y_i$ — внутреннее произведение x и y, где $x = x_1 x_2 \ldots x_n$ и $y = y_1 y_2 \ldots y_n$ for $x_i, y_i \in B(i = 1, 2, \ldots, n)$, и пусть оператор плюс $+$ в состоянии $|x + y\rangle$ будет побитовое сложение по модулю 2.

Далее мы введём некоторые основные квантовые операторы. Положим,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{8.1}$$

— оператор Адамара, действующий на 1-кубитовые состояния $|q\rangle$, и

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{8.2}$$

— оператор «управляемое-НЕ», $CNOT|ct\rangle = |c(t \oplus c)\rangle$ для $c, t \in B$, где c — управляемый бит, и t — целевой бит.

8.1. Квантовый код, исправляющий ошибки

Опишем элементы теории, соответствующей блоковым $[n, k]$ квантовым кодам, исправляющим ошибки (то есть квантовому кодовому слову). Напомним, что в теории кодирования под кодом, исправляющим ошибки, подразумевается код, ошибки определённого типа, возникшие при передаче, исправляются в нём с помощью определённых процедур.

Пусть G — это $k \times n$ порождающая матрица, $\mathrm{C} = \{x | x = vG$ для $v \in \mathrm{B}^k\}$, и $\mathrm{C}^{\perp} = \{y | x \cdot y = 0 \mod 2)$ для $\forall x \in \mathrm{C}$ and $y \in \mathrm{C}\}$.

Положим,

$$|c_w\rangle = \frac{1}{\sqrt{|\mathrm{C}|}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot w} |x\rangle \tag{8.3}$$

— квантовый код (состояние), являющийся блоковым $[n,\ k]$-исправляющим ошибки квантовым кодом для классического кода (слова) $w \in \mathrm{C}$.

Покажем, что этот квантовый код может исправлять два типа ошибок: «bit flip error» $e_1 \in \mathrm{B}^n$ и «phase flip error» $e_2 \in \mathrm{B}^{\mathrm{n}}$.

Действительно, пусть

$$\frac{1}{\sqrt{|\mathrm{C}|}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot (w + e_2)} |x + e_1\rangle \tag{8.4}$$

— повреждённое состояние. Для «bit flip error» мы вначале добавим вспомогательные (ancilla) кубиты $|0^n\rangle$ и применим матрицу проверки чётности H_1 для C, чтобы обнаружить «bit flip error». Так как $\mathrm{H}_1 x = 0$, имеем

$$\frac{1}{\sqrt{|\mathrm{C}|}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot (w+e_2)} |x + e_1\rangle \otimes |\mathrm{H}_1 e_1\rangle. \tag{8.5}$$

Таким образом, мы можем исправить ошибку смены битов («bit flip error»), используя значения вспомогательных (ancilla) кубитов (т. е. синдром), и состояние становится

$$\frac{1}{\sqrt{|C|}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot (w+e_2)} |x\rangle. \tag{8.6}$$

Для ошибки переворота фазы («phase flip error») мы сначала применяем оператор Адамара H к каждому кубиту, и состояние становится

$$\frac{1}{\sqrt{2^n |\mathrm{C}|}} \sum_{z \in \mathrm{B}^{\mathrm{n}}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot (w+z+e_2)} |z\rangle = \frac{1}{\sqrt{2^{\mathrm{n}} |\mathrm{C}|}} \sum_{z \in \mathrm{B}^{\mathrm{n}}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot z'} |w + z' + e_2\rangle =$$

$$= \sqrt{\frac{|\mathrm{C}|}{2^{\mathrm{n}}}} \sum_{z' \in \mathrm{C}^{\perp}} |w + z' + e_2\rangle, \tag{8.7}$$

где $z' = w + z + e_2$, и мы используем свойство, что

$$\sum_{x \in \mathrm{C}} (-1)^{x \cdot z'} = |\mathrm{C}|,$$

если $z' \in \mathrm{C}^{\perp}$, иначе

$$\sum_{x \in \mathrm{C}} (-1)^{x \cdot z'} = 0.$$

Поскольку это состояние может рассматриваться как «bit flip error», мы применяем к состоянию матрицу проверки на чётность H_2 для $\mathrm{C}^{\perp}$ и можем исправить ошибку, используя тот же метод, что упомянут выше. В результате

$$\sqrt{\frac{|\mathrm{C}|}{2^{\mathrm{n}}}} \sum_{z' \in \mathrm{C}^{\perp}} |w + z\rangle. \tag{8.8}$$

Наконец, применив снова H к каждому кубиту, мы можем получить исходное состояние:

$$\sqrt{\frac{|\mathrm{C}|}{2^{2\mathrm{n}}}} \sum_{x \in \mathrm{B}^n} \sum_{z' \in \mathrm{C}^{\perp}} (-1)^{(w+z') \cdot x} |x\rangle = \frac{1}{\sqrt{|\mathrm{C}|}} \sum_{x \in \mathrm{C}} (-1)^{x \cdot w} |x\rangle. \tag{8.9}$$

8.2. Протокол

Алиса и Боб имеют в своём распоряжении ЭПР-пару

$$\frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\Big). \tag{8.10}$$

Алиса рассматривает возможность тайной отправки Бобу сообщения $b \in B$ с использованием стеганографической техники.

Пусть w будет сопроводительным сообщением и состояние $|c_w\rangle$ будет квантовым кодовым словом, соответствующим w и описанным в параграфе 8.1.

Секретное сообщение $b \in B$ встраиваем в контейнер (8.3), комбинируя со сцепленным состоянием (8.10). Получаем стегоконтейнер вида, или квантовое кодовое слово,

$$|c'_w) = \frac{1}{\sqrt{|\mathrm{C}|}}\Big(\sum_{x\in \mathrm{S}_b}(-1)^{x\cdot w}|x\rangle_A \otimes |0\rangle_B + \sum_{x\in \mathrm{S}_{\overline{b}}}(-1)^{x\cdot w}|x\rangle_A \otimes |1\rangle_B\Big) \tag{8.11}$$

вместо квантового кодового слова $|c_w\rangle$, где

$$S_b = \{x | x \in C, \text{когда последний бит у } x \text{ есть } b\}.$$

Убедимся, что Боб может прекрасно исправить кодовое слово, если возникают два типа вышеупомянутых ошибок. Это означает, что ошибки в сопроводительных сообщениях не влияют на восстановление секретного сообщения.

Пусть

$$\frac{1}{\sqrt{|\mathrm{C}|}}\Big(\sum_{x\in \mathrm{S}_b}(-1)^{x\cdot(w+e_2)}|x+e_1\rangle \otimes |0\rangle + \sum_{x\in \mathrm{S}_{\overline{b}}}(-1)^{x\cdot(w+e_2)}|x+e_1\rangle \otimes |1\rangle\Big) \tag{8.12}$$

— такое состояние, в котором имеются два типа ошибок («bit flip error» — ошибка переворачивания битов e_1). Считаем, что ошибки переключения фазы «phase flip error» e_2) возникают, когда Алиса отправляет кодовое слово Бобу.

Во-первых, Боб рассматривает возможность исправления ошибки переворота битов e_1. Он может достичь этого с помощью матрицы контроля чётности H_1, описанной в параграфе 8.1, и получить состояние

$$\frac{1}{\sqrt{|\mathrm{C}|}}\Big(\sum_{x\in \mathrm{S}_b}(-1)^{x\cdot(w+e_2)}|x\rangle \otimes |0\rangle_B + \sum_{x\in \mathrm{S}_{\overline{b}}}(-1)^{x\cdot(w+e_2)}|x\rangle \otimes |1\rangle_B\Big). \tag{8.13}$$

Затем Боб применяет оператор *CNOT* к последнему кубиту в состоянии $|x\rangle$ в качестве управляемого бита и общего кубита Боба в качестве целевого бита (т. е. $|0\rangle_B$ для 1-го слагаемого в (8.13) и $|1\rangle_B$ для 2-го слагаемого), учитывая, что:

$$...\rangle CNOT|b\rangle|0\rangle_B = ...\rangle|b(0\oplus b)\rangle = ...\rangle|bb\rangle = |x\rangle|b\rangle,$$
$$...\rangle CNOT|b\rangle|1\rangle_B = ...\rangle|b(1\oplus \overline{b})\rangle = ...\rangle|b(1\oplus(b\oplus 1))\rangle = |x\rangle|b\rangle.$$

Тогда получаем

$$\frac{1}{\sqrt{|\mathrm{C}|}}\sum_{x\in\mathrm{C}}(-1)^{x\cdot(w+e_2)}|x\rangle\otimes|b\rangle. \tag{8.14}$$

Наконец, он также может исправить ошибку переворота фазы e_2 по методике, упомянутой в параграфе 8.1, и состояние становится

$$\frac{1}{\sqrt{|\mathrm{C}|}}\sum_{x\in\mathrm{C}}(-1)^{x\cdot w}|x\rangle\otimes|b\rangle=|c_w\rangle\otimes|b\rangle. \tag{8.15}$$

Состояние в формуле (8.15), за исключением кубита $|b\rangle$, совпадает с состоянием в формуле (8.3). Поэтому Боб может отдельно получить секретный бит b и сопроводительное сообщение w.

Кроме того, Алиса рассматривает возможность тайной отправки кубита $\alpha|0\rangle+\beta|1\rangle$ Бобу, где α и β — комплексные числа, удовлетворяющие $|\alpha|^2+|\beta|^2=1$. Для этого мы должны выполнить процедуру, проделанную ранее, если сможем создать следующее состояние:

$$|c'_w\rangle=\frac{1}{\sqrt{|\mathrm{C}|}}\Bigg(\alpha\Bigg(\sum_{x\in\mathrm{S}_0}(-1)^{x\cdot w}|x\rangle_A\otimes|0\rangle_B+\sum_{x\in\mathrm{S}_1}(-1)^{x\cdot w}|x\rangle_A\otimes|1\rangle_B\Bigg)+$$

$$+\beta\Bigg(\sum_{x\in\mathrm{S}_1}(-1)^{x\cdot w}|x\rangle_A\otimes|0\rangle_B+\sum_{x\in\mathrm{S}_0}(-1)^{x\cdot w}|x\rangle_A\otimes|1\rangle_B\Bigg)\Bigg). \tag{8.16}$$

8.3. Секретность и безопасность

Теперь мы рассмотрим секретность и безопасность нашей предлагаемой стеганографии, когда подслушиватель Ева измеряет стегосообщение в уравнении (8.11) и состояние становится либо

$$\frac{1}{\sqrt{|\mathrm{C}|}}\Bigg(\sum_{x\in\mathrm{S}_0}(-1)^{x\cdot w}|x\rangle+\sum_{x\in\mathrm{S}_1}(-1)^{x\cdot w}|x\rangle\Bigg), \tag{8.17}$$

или

$$\frac{1}{\sqrt{|\mathrm{C}|}}\Bigg(\sum_{x\in\mathrm{S}_0}(-1)^{x\cdot w}|x\rangle-\sum_{x\in\mathrm{S}_1}(-1)^{x\cdot w}|x\rangle\Bigg) \tag{8.18}$$

с вероятностью 1/2. В этом случае Ева может рассматривать второй вариант (8.18) как ошибку изменения фазы на последнем кубите. Однако она может сомневаться в этом явлении, если оно повторяется. Чтобы избежать этой ситуации, Алиса и Боб заранее договариваются о случайном списке кубитов для использования в каждой кодировке. Используя этот процесс, они могут произвольно изменить местоположение ошибок фазового переворота. Ева не сможет получить какую-либо информацию о секретном сообщении, потому что она может получить совершенно противоположную информацию из-за процедуры перехода от (8.13) к (8.14) без общего кубита Боба.

9. Протокол, замаскированный под квантовый шум

Представим протокол для сокрытия секретных сообщений в форме синдромов ошибок, маскируя их под шум в кодовом слове, преднамеренно применяя исправляемые ошибки в квантовом коде (2011, [13,14]). Идея такого протокола принадлежит Хулио Хеа-Банаклоху [15].

Отправитель (Алиса) преобразует квантовую информацию в кодовое слово и применяет случайный выбор унитарной операции, используя секретный случайный ключ, которым она делится с получателем (Боб). С помощью ключа Боб может получить информацию, но подслушиватель (Ева) с возможностью контролировать канал, но без секретного ключа, не может отличить сообщение от шума канала.

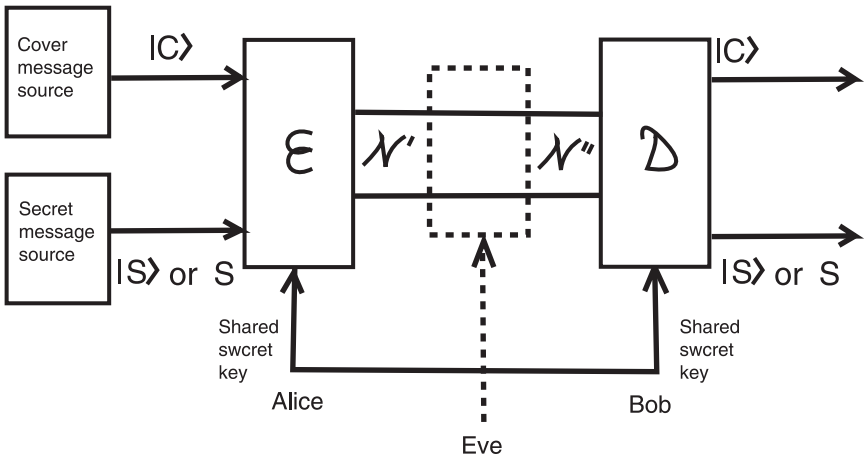

Рис. 7. В стеганографическом кодере $\mathcal{E}$ есть три различных входа: сообщение-контейнер $|C\rangle$; секретное сообщение, которое мы хотели бы скрыть (оно может быть квантовым $|S\rangle$ или классическим S); общий секретный ключ, который может быть квантовым (ebit) $|K\rangle$ или классическим K. Ева может отслеживать некоторую часть шумового квантового канала $\mathcal{N}$, показанного в красном поле. Боб может декодировать стеганографическое сообщение с использованием декодера $\mathcal{D}$ и общего секретного ключа $|K\rangle$ или K и восстанавливать $|C\rangle$ и $|S\rangle$ или S с очень высокой вероятностью [13]

9.1. Протокол Шоу-Бруна

Представим протокол, который достигает вышеуказанных целей. Он имеет следующую структуру:

1) «невинное» квантовое сообщение $|\varphi_c\rangle$ закодировано Алисой в квантовом коде, исправляющем ошибки. Это $|\varphi_c\rangle$ является текстовым контейнером;

2) затем Алиса выполняет вторую операцию над закодированным текстом контейнера, которая встраивает стеганографическое сообщение в кодовое слово. Это стеганографическое сообщение является другим состоянием $|\varphi_s\rangle$ и является стегоконтейнером (Мы называем один бит или кубит стегоконтейнера стегобитом или стегокубитом, соответственно.);

3) модифицированное кодовое слово отправляется по квантовому каналу Бобу, который может (по крайней мере с высокой вероятностью) декодировать его и извлечь текст из стегоконтейнера $|\varphi_s\rangle$;

4) кодирование выполняется таким образом, что, если перехватчик Ева перехватывает кодовое слово, он будет выглядеть точно так же, как закодированное состояние $|\varphi_c\rangle$ после того, как он прошёл через шумовой канал. Другими словами, Ева не может отличить закодированное стеганографическое сообщение от шума в канале.

Мы изображаем общий квантовый стеганографический протокол на рис. 7.

9.2. Квантовый деполяризующий канал

Квантовый аналог классического бинарного симметричного канала является деполяризующим каналом, для которого одной из наиболее широко используемых моделей является:

$$\rho \to \mathcal{N}[\rho] = (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z. \tag{9.1}$$

То есть каждый кубит имеет равную вероятность претерпевать ошибки X, Y или Z. Повторное прохождение кубитом этого канала в конечном итоге отобразит его в максимально смешанное состояние $I/2$. Мы может переписать этот канал в другой, но эквивалентной форме:

$$\mathcal{N} = (1-4p/3)\mathcal{I} + (4p/3)\mathcal{T}, \tag{9.2}$$

где $\mathcal{I}[\rho] = \varrho$ и $\mathcal{T}[\rho] = (1/4)(\rho + X\rho X + Y\rho Y + Z\rho Z)$.

Операция $\mathcal{T}$ является закручиванием (twirling), в ходе которого Алиса применяет одну из четырёх однокубитових операций (гейтов) I, σ_x, σ_y или σ_z к кубиту, определяя конкретную операцию с помощью двух текущих битов ключа. Для злоумышленника, который не имеет ключа, этот кубит выглядит как находящийся в максимально смешанном состоянии (вращение может трактоваться как квантовый шифр Вернама) [16].

Далее Алиса применяет случайные ошибки деполяризации (с использованием тех же однокубитових операций I, σ_x, σ_y или σ_z) к некоторой части других кубитов кодового слова, имитируя тем самым некоторый уровень шума в деполяризующем канале, а затем посылает кодовое слово Бобу. Он использует общий с Алисой секретный ключ, чтобы правильно применить операцию раскручивания (обратная к закручиванию), а затем снова использует ключ для нахождения информационных кубитов [16].

Заметим, что если злоумышленник Ева постоянно мониторит канал в течение длительного периода времени и если у неё есть точное знание свойств канала, тогда она в конечном итоге обнаружит, что Алиса передаёт информацию Бобу с помощью квантового стеганографического протокола. Кроме того, постоянно выполняя квантовые измерения передаваемых состояний кубитов, Ева может предотвратить передачу информации, эффективно затопляя квантовый канал шумом (Атака «отказ в обслуживании») [16].

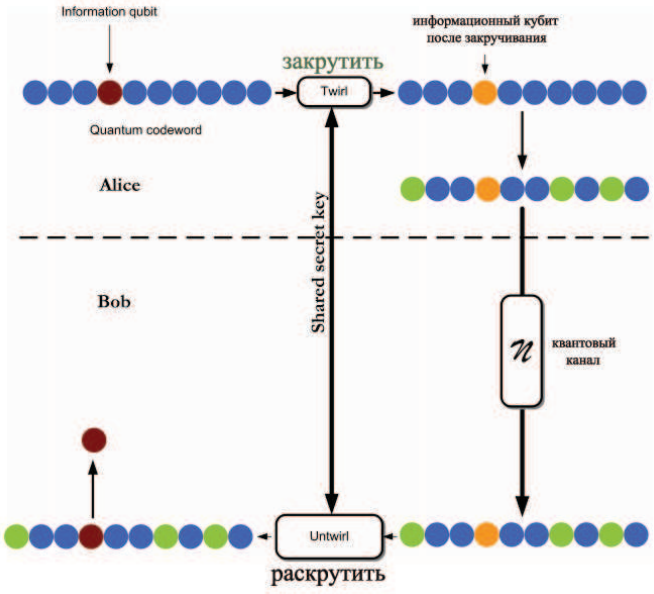

Рис. 8. Алиса скрывает свой информационный кубит (сплошной коричневый круг), заменяя его кубитом своего квантового кодового слова. Она использует свой общий секретный ключ с Бобом, чтобы определить, какой кубит нужно поменять. Она снова использует общий ключ, чтобы закрутить информационный кубит. Кроме того, она применяет случайные деполяризующие ошибки к остальным кубитам кодового слова (показано зелёным цветом). Она отправляет кодовое слово по деполяризующему каналу Бобу, который использует общий секрет, чтобы правильно применить операцию раскручивания, а затем найти и заменить оригинальный информационный кубит Алисы [13]

При рассмотрении канала в этой форме и использовании ошибок X, Y или Z с вероятностью $p/3$, мы можем говорить об удалении кубита с вероятностью $4p/3$ и замене его максимально смешанным состоянием. Эта картина делает стеганографический протокол более прозрачным.

9.3. Канал без шума

Сначала предположим, что фактический физический канал между Алисой и Бобом не имеет шума. Все шумы, которые видит Ева, происходят из-за преднамеренных ошибок, которые Алиса прикладывает к своим кодовым словам. Мы изображаем этот протокол на рис. 8.

Шаг 1. Алиса кодирует текстовый контейнер из k_c кубитов в N кубитов с помощью блокового $[N, k_c]$ квантового кода, исправляющего ошибки.

Шаг 2. Из уравнения (9.2) деполяризующий канал будет максимально смешивать Q кубитов с вероятностью p_Q, где

$$p_Q = \left(\begin{array}{c} N \\ Q \end{array} \right) (4p/3)^Q (1 - 4p/3)^{N-Q}. \tag{9.3}$$

Для больших N Алиса может отправить $M = (4/3)pN(1-\delta)$ стегокубитов, где $1 \gg \delta \gg \sqrt{(1-4p/3)/(4pN/3)}$ (вероятность меньше, чем M ошибок, пренебре-

жимо мала).

Шаг 3. С помощью общего случайного ключа (или общих эбитов) Алиса выбирает случайное подмножество M кубитов из N и заменяет свои M стегокубитов на эти кубиты кодового слова. Она также заменяет случайное число m кубитов вне этого подмножества на максимально смешанные кубиты, так что сумма $Q = M + m$ совпадает с биномиальным распределением, приведённым в формуле (9.3), с высокой точностью.

Шаг 4. Алиса «закручивает» свои стегокубиты, используя $2M$ битов секретного ключа или $2M$ общих эбитов. К каждому кубиту она применяет один из I, X, Y или Z, выбранный случайным образом, поэтому $\rho \to \mathcal{T}\rho$. Для Евы, у которой нет ключа, эти кубиты выглядят максимально смешанными.

Шаг 5. Алиса передаёт кодовое слово Бобу. Из секретного ключа он знает правильное подмножество M кубитов и одноразовый блокнот для их декодирования.

Этот протокол передаёт $(4/3)pN(1-\delta)$ секретных кубитов от Алисы к Бобу (рис. 8).

Секретность следует из таких соображений: без ключа Ева не может отличить стегокубит от максимально смешанного кубита; и эти максимальные кубиты распределены точно так, как и следовало ожидать от деполяризующего канала с частотой ошибок p. Если число p соответствует ожиданиям Евы, она не обнаружит ничего подозрительного, даже если она перехватит кодовое слово и измерит его синдромы ошибок.

9.4. Канал с шумом

Если канал содержит собственный шум, Алиса сначала должна будет кодировать свои k_s стегокубитов в квантовом $[M, k_s]$-коде, исправляющем ошибки, и поменять местами эти M кубитов для случайного подмножества из M кубитов в кодовом слове и применить процедуру закручивания. Это закручивание не влияет на мощность исправления ошибок, если Боб знает ключ. Скорость передачи k_s/N будет зависеть от скорости в квантовом коде, исправляющем ошибки, используемой для защиты стегокубитов. Для бинарного симметричного канала это было бы в лучшем случае $(1-\delta)[1-h(p)]\delta p/(1-2p)$. Однако для большинства квантовых каналов (включая постоянный ток) достижимая скорость неизвестна. Предполагая, что физический канал также является деполяризующим каналом с частотой ошибок p и что Алиса эмулирует деполяризующий канал с частотой ошибок q, эффективный канал будет выглядеть для Евы как деполяризующий канал с частотой ошибок $p + q(1-4p/3) \equiv p + \delta p$. Пока $p+\delta p$ достаточно близко к ожидаемому Евой уровню ошибок, связь будет оставаться секретной. Скорость передачи составляет $k_s/N \approx (4/3)c\delta p/(1-4p/3)$, где $c = k_s/M$ — достижимая скорость кода для деполяризирующего канала с частотой ошибок p.

Секретный ключ используется в двух шагах этих протоколов. Первый на Шаге 3: Алиса выбирает случайное подмножество M кубитов из N-кубитного кодового слова. Имеются C_N^M подмножеств, поэтому для выбора одного из них

необходимо примерно $\log_2 C_N^M$ бита. Затем, на Шаге 4, $2M$ битов ключа используются для закручивания. Это даёт нам

$$n_k \approx \log_2 \left(\begin{array}{c} N \\ M \end{array} \right) + 2M \tag{9.4}$$

бит используемого секретного ключа. Чтобы знать число битов ключа, использованных на кубит, который Алиса посылает через канал, определим степень потребления ключа $K = n_k/N$. Мы используем $M \approx 4qN/3$ и $q \approx \delta p/(1 - 4p/3)$ для выражения K через p, δp и N ([13], рис. 3):

$$K \approx \log_2[(4/\beta)^\beta (1 - \beta N)^{\beta-1}], \quad \beta \equiv 4\delta p/(3 - 4p), \tag{9.5}$$

где δp является дополнительным неконтролируемым шумом в бинарном симметричном канале.

Алиса может использовать меньше битов ключа, если у неё есть источник, который усредняется до максимально смешанного состояния — например, если Алиса сначала сжимает состояние $|\varphi_s\rangle$ перед его отправкой. Это позволило бы обойти процедуру закручивания. Тем не менее, хотя критерий секретности всё ещё может быть соблюдён без закручивания, безопасность не будет соблюдена: если Ева узнает о сообщении, она сможет прочитать его без ключа.

Литература

1. Саватеев Е.О. Построение стеганографической системы на базе протокола IPv4. URL: `https://www.securitylab.ru/contest/264960.php`.
2. Василиу Е.В., Лимарь И.В. Становление и современное состояние квантовых методов защиты информации // Проблемы инфокоммуникаций. (Беларусь). 2016. № 2(4). С. 30–35.
3. Холево А.С. Квантовые системы, каналы, информация. Москва : МЦНМО, 2010.
4. Грибунин В.Г. Оков И.Н., Туринцев И.В. Цифровая стеганография. М. : Солон-Пресс, 2002. 2264 с.
5. Ульянов С.В., Петров С.П. Квантовое распознавание лиц и квантовая визуальная криптография: модели и алгоритмы // Электронный журнал «Системный анализ в науке и образовании». 2012. Вып. 1. С. 1–17.
6. Qu Zh., Li Zh., Xu G., Wu S., Wang X. Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm // IEEE Access. 2019. V. 7. P. 50849–50857.
7. Zhang Y., Lu K., Gao Y., Xu K. A novel quantum representation for log-polar images // Quantum Inf. Process. 2013. V. 12, No. 9. P. 3103–3126.
8. Mihara T. Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data // Journal of Quantum Information Science. 2012. V. 2. P. 10–14. URL: `http://dx.doi.org/10.4236/jqis.2012.21003`. Published Online March 2012 (`http://www.SciRP.org/journal/jqis`).
9. Mihara T. Quantum steganography using prior entanglement // Physics Letters A. 2015. V. 379. P. 952-–955.

10. El Allati A., Ould Medeni M.B., Hassouni Y. Quantum Steganography via Greenberger–Horne–Zeilinger GHZ4 State // Commun. Theor. Phys. 2012. V. 57. P. 577–582.
11. Xu Shu-Jiang. Steganalysis and improvement of a quantum steganography protocol via a GHZ_4 state // Chin. Phys. B. 2013. V. 22, No. 6. P. 060307.
12. Mermin N.D. Deconstructing dense coding // Phys. Rev. A. 2002. V. 66. P. 132308.
13. Shaw B.A., Brun T.A. Quantum steganography with noisy quantum channels // Physical review A. 2011. V. 83. P. 022310-1–022310-8.
14. Shaw B.A., Brun T.A. Quantum steganography. URL: `https://arxiv.org/pdf/1006.1934v1.pdf`.
15. Gea-Banacloche J. Hiding messages in quantum data // J. Math. Phys. 2002. V. 43. P. 4531–4536.
16. Конахович Г.Ф., Шевченко О.В., Кинзерявий В.М., Хохлачова Ю.Е. (НАУ) Сучасні методи квантової стеганографії // Науково-технічний журнал «Захист інформації». 2011. № 2. С. 5–9.

THE PROTOCOLS OF QUANTUM STEGANOGRAPHY

D.E. Vilhovsky
Instructor, e-mail: vilkhovskiy@gmail.com
A.K. Guts
Dr.Sc. (Phys.-Math.), Professor, e-mail: guts@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The purpose of this article is to present methods of modern quantum steganography and make a short review of different types of quantum steganography protocols.

Keywords: quantum steganography, hidden secret data, quantum communication, entangled states.

References

1. Savateev E.O. Postroenie steganograficheskoy sistemi na baze protokola IPv4. URL: `https://www.securitylab.ru/contest/264960.php`. (in Russian)
2. Vasiliu E.V. and Limar' I.V. Stanovlenie i sovremennoe sostoyanie kvantovih metodov zaschiti inforacii. Problimi infokommunikaciy (Belarys'), 2016, no. 2(4), pp. 30–35. (in Russian)
3. Holevo A.S. Kvantovie sistemi, kanali, informatsiya. Moscow, MTsNMO Publ., 2010.
4. Gribunin V.G., Okov I.N., and Turintsev I.V. Tsifrovaya steganografiya. Moscow, Solon-Press, 2002, 264 p. (in Russian)
5. Ul'yanov S.V. and Petrov S.P. Kvantovoe raspoznavanie lits i kvantovaya kriptografiya: modeli i algoritmi. Elektronniy zhurnal "Sistemniy analiz v nauke i obrazovanii", 2012, no. 1, pp. 1–17. (in Russian)

6. Qu Zh., Li Zh., Xu G., Wu S., and Wang X. Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm. IEEE Access, 2019, vol. 7, pp. 50849–50857.
7. Zhang Y., Lu K., Gao Y., and Xu K. A novel quantum representation for log-polar images. Quantum Inf. Process, 2013, vol. 12, no. 9, pp. 3103–3126.
8. Mihara T. Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data. Journal of Quantum Information Science, 2012, vol. 2, pp. 10–14. URL: `http://dx.doi.org/10.4236/jqis.2012.21003`. Published Online March 2012 (`http://www.SciRP.org/journal/jqis`).
9. Mihara T. Quantum steganography using prior entanglement. Physics Letters A., 2015, vol. 379, pp. 952-–955.
10. El Allati A., Ould Medeni M.B., and Hassouni Y. Quantum Steganography via Greenberger–Horne–Zeilinger GHZ4 State. Commun. Theor. Phys., 2012, vol. 57, pp. 577–582.
11. Xu Shu-Jiang. Steganalysis and improvement of a quantum steganography protocol via a GHZ_4 state. Chin. Phys. B., 2013, vol. 22, no. 6, pp. 060307.
12. Mermin N.D. Deconstructing dense coding. Phys. Rev. A., 2002, vol. 66, pp. 132308.
13. Shaw B.A. and Brun T.A. Quantum steganography with noisy quantum channels. Physical review A., 2011, vol. 83, pp. 022310-1–022310-8.
14. Shaw B.A. and Brun T.A. Quantum steganography. URL: `https://arxiv.org/pdf/1006.1934v1.pdf`.
15. Gea-Banacloche J. Hiding messages in quantum data. J. Math. Phys., 2002, vol. 43, pp. 4531–4536.
16. Kohanovich G.F., Shevchenko O.V., Kinzeryaviy V.M., and Hohlachova Yu.E. Suchasni metodi kvantovoi steganografii. Naukovo-tehnichniy zhurnal "Zahist informatii", 2011, no. 2, pp. 5–9. (in Ukrainian)

Дата поступления в редакцию: 27.05.2020