УДК 004.056.55

Введение в квантовую криптографию: основные понятия, подходы и алгоритмы

© Е.Ю. Иванова, Е.А. Ларионцева

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Приведен минимальный набор понятий квантовой физики, необходимых для понимания идей и средств квантовой криптографии. Описаны приоритетные направления развития систем распределения ключей квантовой криптографии, базирующиеся на кодировании квантового состояния одиночной частицы. На основе законов квантовой механики описано построение безопасных протоколов передачи информации, называемых квантовыми протоколами передачи информации. Рассмотрены наиболее популярные на данный момент квантовые протоколы передачи информации BB84 и B92.

Ключевые слова: *квантовая теория информации, квантовая криптография, квантовое распределение ключей.*

Введение. Базовой задачей криптографии является сокрытие данных, как правило, путем их шифрования. Со временем криптография стала решать и другие задачи, близкие к шифрованию по методам решения, например такие, как задачи генерации и распределения ключей, задача аутентификации сторон и т. п. При этом согласованные действия пользователей, результатом которых является решение подобных задач, называют *криптографическими протоколами* [1].

В начале XX в. обнаружилась тесная взаимосвязь между информатикой и физикой. Успех в решении многих задач, которые на первый взгляд имеют отношение только к информационным технологиям и защите информации, может быть достигнут сугубо физическим путем. Перед учеными встали два основных вопроса [2]: насколько велики возможности квантовых алгоритмов? возможно ли создание устройств, реализующих эти алгоритмы?

В 60-е годы XX в., когда бурными темпами начали развиваться информационные технологии и вычислительная техника, зародилась новая наука — квантовая теория информации. Она изучает квантовомеханические состояния и их способность участвовать в процессе переноса и обработки информации. Квантовая теория является математической моделью современного представления о физических свойствах окружающего мира и физических систем, из которых он состоит [3].

Судя по результатам исследований, проводимых в области квантовой теории информации, и анализа квантовых систем, которые уже удается строить на практике, квантовая теория информации имеет блестящие перспективы в криптографии, охватывая весьма обширный ряд задач этой области. В основе этих новых методик лежат особенности квантовой природы канала, однако применение новых принципов и методики защиты информации имеет ряд недостатков, которые будут рассмотрены в данной статье.

Основные понятия квантовой теории информации. Квантовая теория информации работает с квантовыми явлениями, изучает их свойства и закономерности. Главные понятия, на которых строится эта наука, — это квантовые состояния и волновые функции. На их основе формируются такие понятия, как кубит, коллапс волновой функции и запрет клонирования.

Остановимся на каждом из упомянутых понятий более подробно.

Существуют значительные отличия между квантовой и обычной теорией информации. Прежде всего различаются понятия квантовой частицы и макрочастицы. Если в классической физике для частицы, рассматриваемой в качестве некоторого тела в пространстве, существуют такие характеристики, как координаты, масса и размер, то в квантовой физике для частиц невозможно определить, в какой части пространства они находятся (принцип неопределенности Гейзенберга). Тем не менее оказалось возможным предсказывать их поведение с некоторой вероятностью, описать которое можно лишь после полного отказа от классических физических характеристик системы. Это привело к введению принципиально нового понятия — «квантовое состояние».

Квантовое состояние — это положительный эрмитов оператор в гильбертовом пространстве H с единичным следом. Иначе говоря, это полный набор данных (физических величин), определяющих свойства системы. Данные, которые определяются системой, зависят непосредственно от самой системы.

Описание сложной квантовой системы строится на принципе суперпозиции. Состояние представляет собой векторную величину, которую в квантовой теории обозначают символом $|\psi_i\rangle$. Данные обозначения были введены Дираком. Сопряженное состояние, которое используется в скалярном произведении, обозначают символом $\langle\psi_i|$. Тогда скалярное произведение записывается как $\langle\psi_i|\psi_j\rangle$. Для введенных векторов определены операции умножения на число и сложения между собой, например: $c = k_1|a_1\rangle + k_2|a_2\rangle$.

Квантовые состояния подразделяют на два вида: чистые и смешанные. *Чистым квантовым состоянием* называют вектор в гильбертовом пространстве $\mathcal{H}$ с единичной нормой, т. е. $\|\psi\| = \sqrt{(\psi,\psi)}, \psi \in \mathcal{H}$. Для каждого чистого квантового состояния определен оператор плотности $\rho = |\psi_i\rangle\langle\psi_i|$, имеющий единичный след и ранг, равный 1. Данный оператор действует как проектор на чистое квантовое состояние.

В свою очередь, *смешанное квантовое состояние* — это статистическая смесь нескольких чистых состояний, т. е. чистых состояний с соответствующими вероятностями:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \;\; p_i \geq 0 \;\forall i, \;\; \sum_i p_i = 1.$$

Ключевым аспектом в квантовой теории информации является теорема Шредингера. В классическом виде она может быть сформулирована как $i\hbar \dfrac{d|\psi\rangle}{dt} = H|\psi\rangle$. Однако в силу соответствия между эрмитовым и унитарным оператором $U = e^{iH}$ теорема принимает следующий вид: $|\psi'\rangle = U|\psi\rangle$. Данное представление демонстрирует важное свойство квантовых систем, которое используется при построении квантовых каналов передачи информации, а именно: любое изменение в системе может быть описано унитарным оператором.

Примером квантового объекта могут быть системы, состоящие из двух базисных состояний. Тогда гильбертово пространство имеет размерность 2 и обозначается $\mathcal{H}^2$. Примером такой системы может быть система с состояниями $|0\rangle$ и $|1\rangle$ в качестве базисных. Данная система носит название «*кубит*» (квантовый бит).

Любое состояние кубита в произвольный момент времени может быть записано следующим образом: $|\psi\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle$.

Ранг оператора плотности ρ равен 1 для чистых квантовых состояний и 2 для смешанных, которые могут быть представлены как статистическая смесь двух ортогональных состояний:

$$\rho = p|\psi\rangle\langle\psi| + (1-p)|\psi_\perp\rangle\langle\psi_\perp|.$$

Следует непременно рассмотреть такое явление, как коллапс волновой функции. Под *коллапсом волновой функции* (или *редукцией фон Неймана*) понимается мгновенное изменение волновой функции объекта, происходящее при его измерении. Пусть $\{M_i\}$ — текущее измерение, i — полученный результат. Отсюда исходное состояние в результате проведенного измерения будет преобразова-

но в $\rho_i' = \dfrac{\sqrt{M_i}\rho\sqrt{M_i}}{\mathrm{Tr}M_i\rho}$. Данное утверждение свидетельствует о том, что попытки измерить состояние системы ведут к помехам в ней, а значит, к возникновению ошибок на стороне приемника, которые можно легко обнаружить. Это поведение системы очень удобно и важно в криптографии.

Неортогональные квантовые состояния обладают еще одним важным свойством — *невозможностью (запретом) их клонирования*. Потребность в клонировании состояний может возникнуть, например, у злоумышленника, пытающегося собрать полную статистику результатов измерений.

Приведем пример, показывающий невозможность клонирования состояний. Под преобразованием U, клонирующим некоторое чистое квантовое состояние $|\psi\rangle$, понимается следующее преобразование: $U|\psi\rangle\otimes|A\rangle = |\psi\rangle\otimes|\psi\rangle$ (как было показано ранее, любое преобразование квантовой системы можно описать унитарным оператором). В этой формуле $|A\rangle$ — исходное состояние вспомогательной системы.

Рассмотрим действие данного преобразования на квантовые состояния $|0\rangle$ и $|1\rangle$ и состояние $\dfrac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$:

$$U|0\rangle\otimes|A\rangle = |0\rangle\otimes|0\rangle, \tag{1}$$

$$U|1\rangle\otimes|A\rangle = |1\rangle\otimes|1\rangle. \tag{2}$$

Так как оператор U линейный, то на основании формул (1) и (2) получаем

$$U\left(\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right)\otimes|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle\right).$$

С другой стороны, согласно определению U имеет место соотношение

$$U\left(\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right)\otimes|A\rangle = \frac{1}{2}\left(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle\right).$$

Получаем противоречие, значит, первоначальное предположение о возможности клонирования неортогональных состояний ошибочно.

Квантовый протокол BB84. Идея использования квантовых объектов для защиты информации от подделки и несанкционированного доступа впервые была высказана Стефаном Вейснером в 1970 г.

В 1980 г. Чарльз Беннет и Жиль Брассард, ознакомившись с трудами Вейснера, высказали предположение о возможности применения квантовых объектов для передачи секретного ключа. В 1984 г. в статье они предложили использовать квантовый протокол BB84 для распределения ключей.

Схема передачи ключа посредствам данного протокола приведена далее.

Протокол использует четыре квантовых состояния, образующие два базиса, например поляризационные состояния света (рис. 1). Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно неортогональными, что необходимо для определения возможных попыток нелигитимного съема информации. Таким образом, носителями информации в протоколе BB84 являются фотоны, поляризованные под углами 0, 45, 90, 135º. С помощью некоторого измерения можно различить только два ортогональных состояния: 1) фотон поляризован вертикально или горизонтально; 2) фотон поляризован под углами 45 и 135º. Однако отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45º, невозможно.

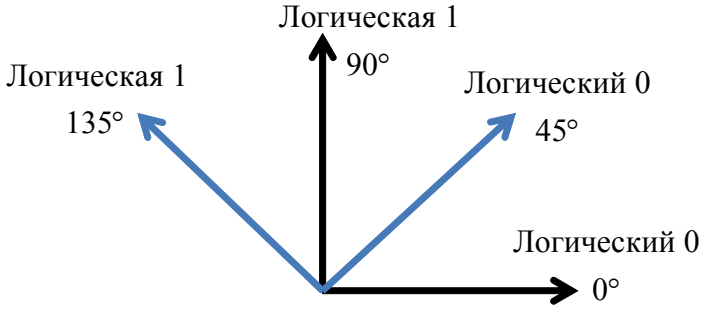

Рис. 1. Выбор базисов [4]

Кодирование состояний осуществляется следующим образом:

- $|0\rangle$
  - $|\leftrightarrow\rangle$
  - $|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + |\leftrightarrow\rangle\right)$
- $|1\rangle$
  - $|\updownarrow\rangle$
  - $|\nwarrow\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle - |\leftrightarrow\rangle\right)$

Пусть пользователь Алиса хочет передать пользователю Бобу некоторую информацию. Тогда они осуществляют следующие действия:

1. Алиса посылает Бобу бит, задавая квантовые состояния — поляризацию в 0, 45, 90 и 135º.

2. Боб имеет два анализатора: для распознавания вертикально-горизонтальной и диагональной поляризации. Для каждого фотона Боб случайно выбирает один из анализаторов и записывает его тип и результат измерений.

Полученный ключ верен с вероятностью $P = 75$ %, т. е. содержит ~25 % ошибок.

3. По общедоступному каналу связи Боб сообщает Алисе, какие анализаторы использовались, но не сообщает, какие результаты были получены.

4. Алиса по общедоступному каналу связи сообщает Бобу, какие анализаторы он выбрал правильно. Те фотоны, для которых Боб неверно выбрал анализатор, отбрасываются.

5. Для обнаружения перехвата Алиса и Боб выбирают случайный участок ключа и сравнивают его по общедоступному каналу связи. Если процент ошибок велик, это свидетельствует о перехвате ключа, и процедура повторяется сначала.

Квантовый протокол B92. В 1992 г. Чарльз Беннет предложил протокол, который по существу является упрощенной версией BB84. Он изложил его в статье «Квантовая криптография с использованием любых двух неортогональных состояний» [4]. Основное отличие B92 от BB84 состоит в том, что B92 использует только два состояния против четырех у BB84 [4].

Кодирование состояний осуществляется следующим образом:

- отправитель (рис. 2):
  - $|0\rangle = |\updownarrow\rangle$
  - $|1\rangle = |\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + |\leftrightarrow\rangle\right)$
- получатель:
  - $|0\rangle = |\leftrightarrow\rangle$
  - $|1\rangle = |\nwarrow\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle - |\leftrightarrow\rangle\right)$

Опишем схему протокола. Пусть пользователь Алиса хочет передать пользователю Бобу некоторую информацию. Тогда они осуществляют следующие действия:

1. Алиса посылает Бобу бит, задавая квантовые состояния согласно своему базису — поляризацию в 45 или 90º.

2. Боб имеет два поляризатора — горизонтальный и расположенный под углом 135º. Для каждого фотона Боб случайно выбирает один из поляризаторов и записывает его тип и результат измерений.

3. Если регистратор зафиксировал фотон, значит, плоскость поляризации, выбранная Бобом, расположена под углом 45º к плоскости поляризации фотона. Таким образом может быть произведено декодирование. Если фотон зарегистрирован не был, ничего сказать нельзя.

4. Боб по общедоступному каналу связи сообщает Алисе, какие биты он сумел декодировать, и именно они принимаются как биты будущего ключа.

5. Для обнаружения перехвата Алиса и Боб выбирают случайный участок ключа и сравнивают его по общедоступному каналу связи. Если процент ошибок велик, это свидетельствует о перехвате ключа, и процедура повторяется сначала.

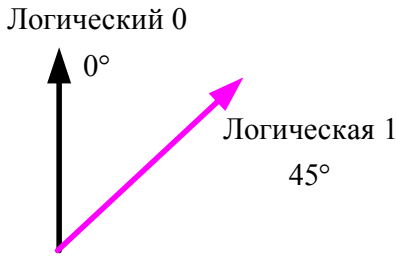

Рис. 2. Базис протокола отправителя B92

Заключение. На данный момент квантовая криптография является единственной альтернативой системам асимметричного шифрования в задаче распределения ключей. Ввиду вышесказанного в случае значительного падения сложности взлома систем асимметричного шифрования квантовая криптография имеет потенциал для развития. Однако высокая технологическая сложность организации систем, использующих принципы и методы квантовой криптографии, не позволяет ей вытеснить асимметричные системы даже при достаточно высоком уровне развития современных технологий.

ЛИТЕРАТУРА

[1] Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. *Квантовая криптография*. Москва, Изд-во МГУ им. М.В. Ломоносова, 2006, с. 23–40.

[2] Вялый М. *Квантовые алгоритмы: возможности и ограничения*. Санкт-Петербург, 2011. URL: http://www.compsciclub.ru/csclub/sites/default/files/20110403_quantum_algorithms_vyali_lecture_notes.pdf (дата обращения 20.10.2013).

[3] *Постулаты квантовой теории*. ВГУ, 2012. URL: http://www.rec.vsu.ru/rus/ecourse/quantcomp/sem2.pdf (дата обращения 18.10.2013).

[4] Bennett C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.,* 1992, vol. 68, no. 21, pp. 3121–3124.

[5] Haitjema M. *A Survey of the Prominent Quantum Key Distribution Protocols*. URL: http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum (дата обращения 18.10.2013).

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Иванова Е.Ю., Ларионцева Е.А. Введение в квантовую криптографию: основные понятия, подходы и алгоритмы. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1000.html

Иванова Екатерина Юрьевна родилась в 1991 г. Студентка кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. e-mail: kat.ivanova@hotmail.com

Ларионцева Евгения Александровна родилась в 1991 г. Студентка кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. e-mail: e.lariontseva@yandex.ru