УДК 003.26:004.056.55:621.39

В.Н. Рудницкий, А.Г. Корченко, С.А. Гнатюк

Черкасский государственный технологический университет, Черкассы

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ КВАНТОВЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОЙ СВЯЗИ

В статье проведен анализ особенностей использования современных квантовых технологий для обеспечения конфиденциальной связи.

Ключевые слова: *квантовые технологии, конфиденциальная связь, квантовый компьютер.*

Введение

Идея точного моделирования явлений квантовой физики на компьютере нового вида – квантовом – впервые была высказана Фейнманом в 1981 г. [1]. Фейнман считал, что было бы естественно моделировать физическую реальность, которая подчиняется квантовым законам, с помощью компьютера, построенного из квантово-механических элементов, подчиняющихся законам квантовой механики. Бурное развитие идеи создания ***квантового компьютера*** началось только с 1994 г., когда П. Шор изобрел первый ***квантовый алгоритм*** факторизации и вычисления дискретного логарифма [2], который экспоненциально быстрее известных классических алгоритмов, предназначенных для традиционных персональных компьютеров. Эффективный алгоритм Шора состоит из квантовой и классической частей. Первая часть представляет собой квантовое решение т.з. задачи нахождения порядка. В этом решении скрыта основополагающая идея, позволяющая факторизовать большое число N за $O\left(\log_2^3(N)\right)$ шагов (вентилей), вместо наиболее известного классического метода, требующего асимптотически

$$O\left(\exp\left[c\cdot\log_2^{\frac{1}{3}}(N)\log_2^{\frac{2}{3}}(\log_2(N))\right]\right) \text{ шагов}$$

(т.е. экспоненциального по $\log_2^{\frac{1}{3}}(N)$ числа), где c – некоторая постоянная. Для факторизации числа с P десятичными знаками любому классическому компьютеру требуется число шагов, которое растет экспоненциально с P. То есть, при добавлении одного десятичного знака к числу в общем случае время факторизации умножается на постоянный множитель, таким образом, при увеличении числа знаков задача быстро становиться не реальной. Наибольшее число, которое было разложено на простые множители в качестве математического соревнования, состояло из 129 знаков. А задачу факторизации числа с 1 000 знаками с помощью классического компьютера, на данный момент, невозможно решить, так как на ее решение понадобилось бы время во много раз больше, чем возраст вселенной. Квантовые компьютеры смогут факторизовать число с 1 000 знаками за долю секунды – и время расчета будет расти только как куб числа знаков. Для лучшего понимания следует отметить, что в классическом компьютере 2 бита – это вдвое больше информации, чем в 1 бите, 8 бит – это соответственно в восемь раз больше. В квантовой вычислительной машине 2 кубита – это уже в четыре раза больше информации, чем в одном, а 8 кубит – это в 128 раз больше.

Чуть позже Л. Гровер создал алгоритм быстрого поиска в неупорядоченной базе данных [1-3], который инициировал лавину новых исследований в области квантовых вычислений во всем мире. Гровер показал, что поиск некоторого уникального значения в неупорядоченной базе из N-элементов на квантовом компьютере может занять $O(\sqrt{N})$ шагов (вентилей), при этом наилучший алгоритм на классическом компьютере может занять $O(\frac{N}{2})$ шагов.

Алгоритм Гровера можно использовать для более быстрого, чем на классическом компьютере, нахождения статистик (наименьшего, среднего, наибольшего элемента). С его помощью можно ускорить алгоритмы решения некоторых задач класса NP – тех задач, для которых не известен лучший алгоритм, чем прямой перебор. Наконец, его применение позволит ускорить поиск ключа к таким криптосистемам как DES, AES и др. Например, для взлома DES нужно найти ключ из $2^{56} \approx 7\cdot 10^{16}$ возможных ключей. Классическому компьютеру в среднем понадобиться $\frac{2^{56}}{2} = 2^{55} \approx 3{,}5\cdot 10^{16}$ шагов. Если их перебирать со скоростью 10^8 ключей в секунду (что не является проблемой для современных вычислительных систем), то классическому компьютеру понадобиться $\frac{3{,}5\cdot 10^{16}}{10^8} = 3{,}5\cdot 10^8$ секунды

или ≈ 11 лет. Квантовому компьютеру, использующему алгоритм Гровера, понадобиться $\sqrt{2^{56}} = 2^{28} \approx \sqrt{7} \cdot 10^8$ шагов, что при переборе со скоростью 10^8 ключей в секунду составит $\frac{\sqrt{7} \cdot 10^8}{10^8} = \sqrt{7} \approx 2,6$ секунд.

Из вышесказанного видно, что современные криптосистемы могут быть уязвимы при использовании квантового компьютера, и поэтому ставится под сомнение использование любых классических криптографических алгоритмов в будущем. На данный момент ведутся активные работы по созданию такого компьютера (если не брать к вниманию уже созданный канадской компанией D-Wave в 2007 г. 16-ти кубитный компьютер Orion), а когда они будут завершены пока не известно. Гипотетично, такие работы может быть уже завершены и квантовые компьютеры проходят последние испытания, а возможно уже и работают в интересах спецслужб.

Основной материал

Схематическая структура типичного квантового компьютера представлена на рис. 1 [2], состоит он из n кубитов и позволяет проводить одно- и двухкубитовые операции над любым из них (или любой парой кубитов).

Эти операции выполняются под воздействием импульсов внешнего поля, управляемого классическим компьютером.

Рис. 1. Структурная схема квантового компьютера

При решении задач на квантовом компьютере ускорение процесса лежит в квантовой природе кубитов. Квантовость кубитов приводит к нескольким феноменам [2, 3]:

1. *Феномен квантового параллелизма*. Гильбертово пространство состояний квантовой системы из *n* кубитов имеет огромную размерность, равную 2^n. Физически это означает, что система имеет 2^n базовых состояний, а состояние компьютера описывается суперпозицией из этих 2^n базовых состояний. При воздействии на какой-либо кубит одновременно изменяются все базовые состояния.

2. *Вычислительный процесс носит характер интерференции,* так как амплитуды базисных состояний являются комплексными числами. Квантовый компьютер можно рассматривать как сложное интерференционное устройство, в котором интерференция состояний создает вычислительную мощь компьютера.

Таким образом, реализация вышеупомянутых квантовых алгоритмов на квантовом компьютере ставит под угрозу конфиденциальность информации, которая передается в зашифрованном виде в информационно-коммуникационных системах.

Алгоритм шифрования DES до недавних пор был государственным стандартом США, сейчас таким является AES, который также основан на вычислительной стойкости, как и большинство алгоритмов, которые обеспечивают секретную связь по всему миру. Таким образом, возникает вопрос о целесообразности использования классических криптоалгоритмов для обеспечения конфиденциальной связи. По информации компании Symantec около 75% предприятий 27 стран мира стали жертвами кибератак и последствия становят близко 2 млн. долларов США с расчета на одно предприятие – исходя из этого, потребность поиска новых средств конфиденциальной связи становится очевидной. Если же посмотреть, как стремительно в нашей стране информатизация охватывает все сферы жизни, то можно смело констатировать, что вышеупомянутая проблема является актуальной и для отечественных предприятий.

На помощь приходят те же квантовые технологии [4, 5], большинство которых основано на передаче информации, закодированной в квантовых состояниях микрочастиц. Особое место в этом списке занимает квантовое распределение ключа (КРК). Отметим, что в большинстве случаев под термином "квантовая криптография" имеется в виду именно "квантовое распределение ключа", хотя некоторые ученые

выделяют несколько направлений квантовой криптографии [6, 7], среди которых и распределение ключа. Для лучшего понимая, приведем глоссарий базовых терминов в этой области. ***Квантовая криптография (Quantum Cryptography)*** – мультидисциплинарное научное направление, которое охватывает методы систем безопасной связи и основывается на незыблемости законов квантовой механики. ***Квантовое распределение ключа (Quantum Key Distribution)*** – это схема распределения ключа с безусловной стойкостью, которая использует поляризационные состояния фотонов. ***Квант (Quantum)*** – элементарная, неделимая порция какой-либо физической величины. ***Фотон (Photon)*** – элементарная частица, квант электромагнитного поля, носитель квантового состояния. ***Кубит (Qubit)*** – двухуровневая квантовая система, квантовый аналог классического бита, который кроме двух классических состояний может еще находится в состоянии суперпозиции. ***Кудит (Qudit)*** – d-уровневая квантовая система, обобщение понятия "кубит" на многоуровневые системы (например, если система трехуровневая – "кутрит", четырехуровневая – "кукварт" и т.д.).

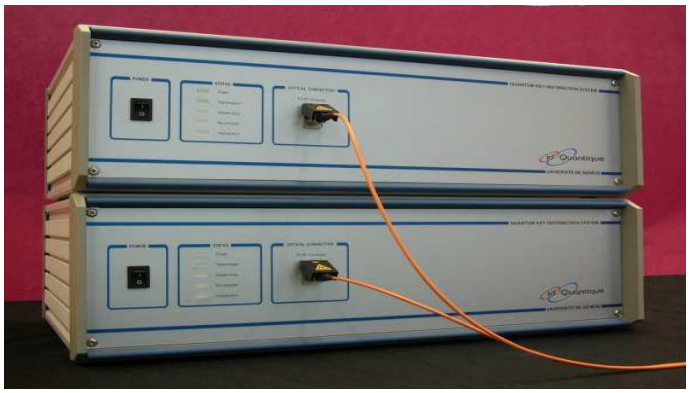
Основными принципами квантовой механики [1 – 7], которые лежат в основе квантовой криптографии, являются: *1) Постулат измерения* (последствие из принципа Гейзенберга), соответственно которому, в результате измерения некоторой физической величины, состояние квантовой системы изменяется – то есть невозможно провести измерения над системой, не изменивши ее. Это правило позволяет обнаружить любое вмешательство в систему третьих лиц. *2) "Теорема о запрете клонирования"* гласит о невозможности копирования произвольного квантового состояния со стороны нарушителя – это делает невозможным создание точных копий состояний фотонов при условии использования любого оборудования.

Незыблемость этих постулатов квантовой механики делает возможным достижения ***безусловной стойкости (unconditional security)*** систем КРК, которая не зависит от вычислительных и других возможностей нарушителей. Это и является основным преимуществом квантовой криптографии над классическим аналогом. Отметим также, что если систему КРК объединить с абсолютно стойкой системой шифрования (например, методом Вернама), то можно сделать абсолютно безопасную систему связи. Эта гибридная система будет также обладать так называемой ***постоянной безопасностью*** – это означает, что сообщение остается абсолютно секретным для злоумышленников, и нет ни единого шанса, что будущий прогресс криптоаналитических и вычислительных средств позволит его расшифровать. К примеру, если же сообщение, зашифрованное любой системой с вычислительной стойкостью, то злоумышленник может сохранять его и ждать появления более совершенных криптоаналитических методов, что очень вероятно произойдет в некоторый момент в будущем, так как это непременно случалось в прошлом.

Протоколы КРК можно классифицировать [4 – 6] по признаку использования некоторой квантовой технологии – это протоколы с использованием *одиночных фотонов (BB84, SARG, с шестью состояниями, "4+2", Гольденберга-Вайдмана, Коаши-Имото и др.), фазового кодирования (B92), переплутаных состояний (E91), кудитов и состояний "приманки"*. Первая технология легла в основу создания практических коммерческих решений в области квантовой криптографии. Например, система QPN Security Gateway (QPN-8505) (рис. 2, б), разработана компанией *MagiQ Technologies* (США), является выгодным решением для правительственных и финансовых организаций [5]. Швейцарская компания *ID Quantique* предлагает на рынке несколько систем, среди которых Clavis и Cerberis (рис. 2, а) – это сервер с автоматической генерацией и секретным обменом ключами через волоконно-оптический канал связи. Не так давно компания *Toshiba Research Europe Ltd* (Великобритания) представила еще одну подобную систему под названием Quantum Key Server. Эта система отличается простотой архитектуры и обеспечивает генерацию ключей и их передачу между пользователями. Другая британская компания *QinetiQ* предлагает первую в мире сеть, которая использует квантовую криптографию – Quantum Net (Qnet) [5].

Заключение

Научные сотрудники ведущих мировых исследовательских центров (Northwestern University, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, Национальная лаборатория в Лос-Аламосе и др.) принимают активное участие в реализации проектов, таких как *SECOQC (Secure Communication based on Quantum Cryptography)* и *EQCSPOT (European Quantum Cryptography and Single Photon Technologies)* [5]. Успешные эксперименты ученых таких стран как США, Швейцария, Австрия, Канада, Япония и Китай констатируют фантастические возможности квантовой криптографии в решении сложных задач информационной безопасности. Что касается Украины, то на данный момент исследования проводятся всего несколькими научными группами *(в Национальном авиационном университете, Одесской национальной академии связи им. Попова, Институте физики НАН Украины)* и, при отсутствии экспериментальной базы и серьезного финансирования фундаментальных исследований, скорей всего, отечественному потребителю придется пользоваться дорогими импортными системами.



а

б

Рис. 2. Системы квантовой криптографии: а) Cerberis от ID Quantique; б) QPN от MagiQ

Список литературы

1. *Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М. : Мир, 2006. – 824 с.*

2. *Физика квантовой информации : Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Ред. Д. Боумейстер [и др.] ; пер. с англ. С.П. Кулик, Е.А. Шапиро ; ред. пер. С.П. Кулик, Т.А. Шмаонов. – М. : Постмаркет, 2002. – С. 33-73.*

3. *Гомонай О.В. Лекції з квантової інформатики: навчальний посібник / О.В. Гомонай. – Вінниця: О. Власюк, 2006. – С. 62.*

4. *Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius : Technika. – 2010. – Vol. 14, № 2. – P. 58-69.*

5. *Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. – 2010. – № 1. – С. 77-89.*

6. *Румянцев К.Е. Квантовая связь и криптография: Учебное пособие / К.Е. Румянцев, Д.М. Голубчиков. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – 122 с.*

7. *Килин С.Я. Квантовая криптография : Идеи и практика: монография / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. – Мн., 2008. – 398 с.*

Поступила в редколлегию 25.05.2011

Рецензент: д-р техн. наук, проф. И.В. Шостак, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ КВАНТОВИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОГО ЗВ'ЯЗКУ

В.М. Рудницький, А.Г. Корченко, С.А. Гнатюк

Стаття присвячена аналізу особливостей використання сучасних квантових технологій для забезпечення конфіденційного зв'язку.

Ключові слова: *квантові технології, конфіденційний зв'язок, квантовий комп'ютер.*

FEATURES OF THE USE OF MODERN QUANTUM TECHNOLOGIES FOR PROVIDING OF CONFIDENTIAL CONNECTION

V.N. Rudnitskiy, A.G. Korchenko, S.A. Gnatyuk

The article is devoted the analysis of features of the use of modern quantum technologies for providing of confidential connection.

Keywords: *quantum technologies, confidential connection, quantum computer.*