АНАЛИЗ ИСПОЛЬЗОВАНИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ В КРИПТОГРАФИИ

М.А. Шемякина, *магистрант*
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты (Россия, г. Шахты)

DOI: 10.24411/2500-1000-2019-11012

Аннотация. *В данной статье приведен анализ использования квантовых вычислений в криптографии. Показаны основные угрозы для информационной безопасности, которые кроются в квантовых вычислениях. После создания полноценного квантового компьютера алгоритм шифрования RSA будет дискредитирован квантовым алгоритмом Шора. Рассмотрены основные направления развития квантовой криптографии: квантовые каналы связи и протокол обмена ключами.*

Ключевые слова: *квантовые вычисления, информационная безопасность, квантовая криптография, квантовые алгоритмы, протокол обмена ключами.*

Любая деятельность современного человека неотъемлемо связана с информацией. На данный момент она является стратегическим ресурсом общества, требующим надежные методы защиты от несанкционированного доступа. Однако, несмотря на большое количество существующих способов обеспечения защиты информации, регулярно возникают новые угрозы для информационной безопасности. Одна из таких угроз – квантовые вычисления, которые, как бы парадоксально это не звучало, одновременно с угрозой предоставляют новые способы защиты информации, породив новое направление в информационной безопасности – квантовую криптографию.

В основе квантовой информатики и квантовых вычислений лежит понятие квантового бита (кубит), который является в некотором роде аналогом классического бита. Особенностью кубита является то, что он может находиться в состоянии суперпозиции. Суперпозиция состояний представляет собой линейную комбинацию состояний квантового бита [1, с. 34]. При выполнении унитарных операций над n-кубитовой квантовой системой, которая находится в состоянии суперпозиции, происходит одновременная обработка всех 2^n возможных состояний. Именно этот эффект, который получил название квантовый параллелизм, позволяет хранить большое количество информации и дает значительное ускорение вычислительного процесса. Для решения практических задач компьютер, основанный на использовании эффекта суперпозиции, должен иметь квантовый регистр, который состоит из 1000 кубитов [2], что эквивалентно примерно 10^{301} классических битов. О фундаментальных принципах квантовых вычислений подробно описано в [1].

Квантовые вычисления как угроза информационной безопасности. На сегодняшний день большая часть информации, которая передается по каналам передачи данных, шифруется с использованием криптографических систем с открытым ключом. Принцип работы данных систем заключается в использовании двух ключей. Открытый ключ используют при шифровании исходного сообщения. Он публикуется в открытом доступе. Закрытый или секретный ключ используют при расшифровке полученного сообщения. С конца 70-х годов прошлого века наиболее часто используемой системой с открытым ключом является алгоритм RSA.

Кратко рассмотрим принцип работы данного алгоритма (рис. 1). При шифровании сообщения оно возводится в степень по модулю N. Полученное зашифрованное сообщение передается по незащищенным каналам связи. Чтобы расшифровать полученное сообщение, нужно использовать функцию Эйлера от числа N, для чего необходимо знать простые множители N. Более подробно принцип действия алгоритма RSA описан в [3]. Таким образом,

для дешифровки сообщения злоумышленнику необходимо факторизовать число N.

В криптографии для удобства приняты следующие обозначения, отправитель – Алиса, получатель – Боб, злоумышленник – Ева.

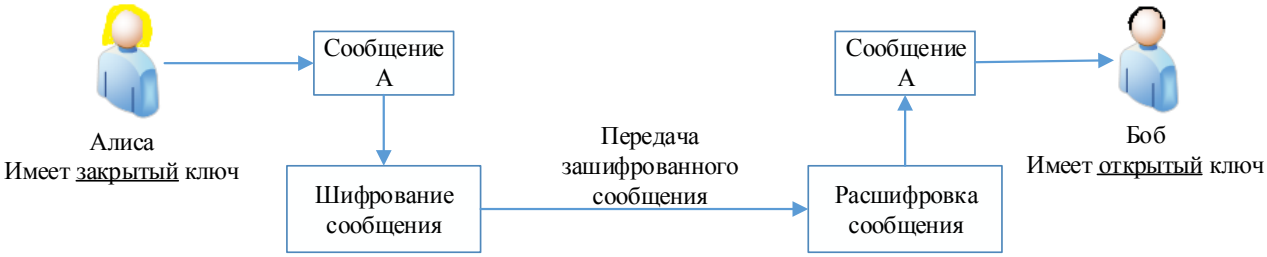

Рис. 1. Алиса передает сообщение А Бобу

Стойкость алгоритма RSA основывается на том, что факторизация больших чисел – очень сложная математическая задача, для которой до сих про не существует эффективного алгоритма решения. Именно поэтому данная криптографическая система с открытым ключом долгое время считалась одной из самых надежных из всех систем шифрования.

Однако в 1994 года американский ученый Питер Шор разработал квантовый алгоритм факторизации (алгоритм Шора). Полученный квантовый алгоритм, в отличии от классических алгоритмов, справляется с задачей факторизации за полиномиальное время. Исходя из этого факта алгоритм Шора может быть использован для взлома RSA. Таким образом, как только будет создан квантовый компьютер, состоящий из 1000 кубитов и более, вся информация, зашифрованная алгоритмом RSA будет моментально скомпрометирована, что поставит под угрозу информационную безопасность общества и в частности криптографию.

Использование квантовых вычислений как средство защиты информации. Угроза квантовых вычислений породила новые подходы к защите информации. Первый подход – постквантовая криптография – предлагает использовать алгоритмы шифрования, базирующиеся на математических задачах, которые сложны как для классических вычислений, так и для квантовых. Второй подход – квантовая криптография – для обеспечения секретности информации использует основные законы квантовой механики. В квантовой криптографии можно выделить следующие основные направления: технологии квантовой передачи данных; технологии квантового распределения ключей; квантовое шифрование; технологии квантовой цифровой подписи, технологии квантового хеширования.

Математически было доказано, что квантовые каналы передачи данных являются самыми безопасными, что позволяет получить новый уровень защиты информации. Носителем информации, которая зашифрована с использованием законов квантовой механики, в данном случае будет квантовый объект, например, фотон. Согласно фундаментальным законам квантовой физики измерение квантового объекта или любое другое воздействие на него приводит к изменению его состояния. Из этого следует, что попытка перехватить сообщение или прослушивание канала приведет к изменению состояния фотона, что сразу же станет известно получателю.

Квантовые каналы передачи данных являются основой для реализации алгоритмов квантового распределения ключей – главного направления развития квантовой криптографии.

Технология квантового распределения ключей (далее – КРК) позволяет распределять ключи между удаленными пользователями по открытым каналам связи, основываясь на законах квантовой физики. Технология КРК строится на невозможности копирования неизвестного квантового состояния; невозможности прослушать сигнал; невозможности абсолютно надеж-

но различить два неортогональных квантовых состояния.

Все протоколы КРК работают по следующему принципу: Алиса (отправитель) задает квантовые состояния фотонов и передает по квантовым каналам передачи данных. Боб (получатель) получает фотоны и регистрирует их состояния. Если Алиса и Боб заранее не договорились, какой вид поляризации фотонов будет выбран, тогда Боб разрушит полученный сигнал. Имело ли место прослушивание при передаче ключа Алиса и Боб смогут определить, сравнивая переданные и полученные данные. Метод сравнения определяется каждым протоколом КРК.

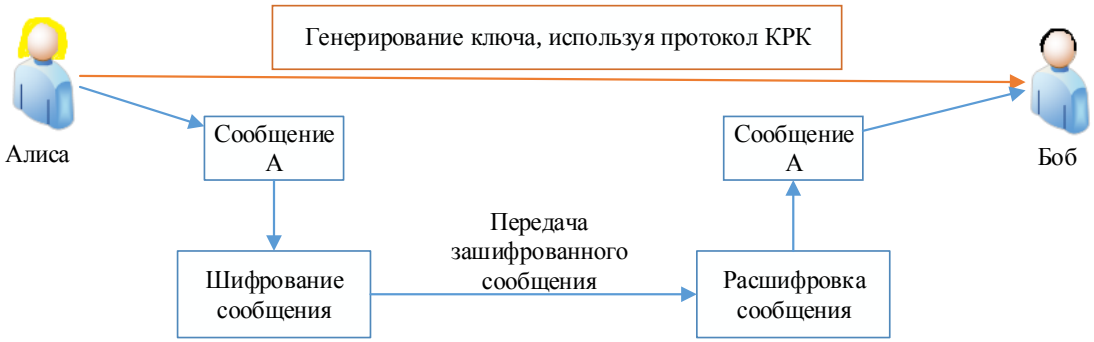

Рис. 2. Алиса передает сообщение А Бобу

Главным требованием к абсолютно стойким шифрам заключается в том, что ключ для него должен быть равен по длине или превосходить длину кодируемого сообщения [4]. Однако учеными было доказано, что в квантовой криптографии ключ может быть короче самого сообщения. Была реализована абсолютно стойкая система квантового шифрования, которая позволяет передавать шесть бит информации в каждом фотоне, при этом длина ключа меньше чем длина сообщения. Это позволяет передавать новый ключ внутри основного сообщения. Подробно технология абсолютно стойкого шифрования описана в [5].

Заключение. В данной работе был проведен анализ использования квантовых технологий в области информационной безопасности. В результате анализа было выявлено, что после создания квантового компьютера классическая криптография станет неэффективным способом защиты информации. Именно поэтому возник новый подход к защите информации – квантовая криптография. Квантовая криптография является бурно развивающейся отраслью информационной безопасности. Многие государства, в том числе и Россия, вкладывают большие деньги в развитие этого направления и решение технических проблем. Опираясь на законы физики, квантовая криптография является одним из самых надежных способов защиты информации.

Библиографический список

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

2. *Корольков А.В.* О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы квантовой кибербезопасности – 2015. – № 1 (9). – С. 6–13.

3. *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 328 с.

4. *Квантовая криптография* / шифрование. – [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_(%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) (дата обращения: 21.05.2019).

5. *Стойкое квантовое шифрование* – будущее информационной безопасности. – [Электронный ресурс]. – Режим доступа: http://integral-russia.ru/2016/06/10/stojkoe-kvantovoe-shifrovanie-budushhee-informatsionnoj-bezopasnosti/ (дата обращения: 25.05.2019).

ANALYSIS OF THE USE OF QUANTUM TECHNOLOGIES IN CRYPTOGRAPHY

M.A. Shemyakina, *graduate student*
Institute of service and entrepreneurship (branch) of DSTU in Shakhty
(Russia, Shakhty)

Abstract*. This article analyzes the use of quantum computing in cryptography. The main threats to information security that are rooted in quantum computing are shown. After creating a full-fledged quantum computer, the RSA encryption algorithm will be discredited by the Shore quantum algorithm. The main directions of development of quantum cryptography are considered: quantum communication channels and key exchange protocol.*

Keywords*: quantum computing, information security, quantum cryptography, quantum algorithms, key exchange protocol.*