УДК 004.716
DOI: 10.33764/2618-981X-2021-6-78-83

# ТЕХНОЛОГИИ КВАНТОВОЙ КРИПТОГРАФИИ

***Евгений Александрович Долгочуб***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (913)932-07-05, e-mail: evgeniidolg@mail.ru

***Алексей Николаевич Поликанин***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (913)397-63-51, e-mail: polikanin.an@yandex.ru

В статье рассмотрены основные классические алгоритмы квантовой криптографии, объясняющие принцип работы механизма обеспечения информационной безопасности при передаче сообщений с анализом поляризации фотонов. Сделаны выводы о наиболее оптимальных вариантах сочетания алгоритмов.

**Ключевые слова:** квантовая криптография, дешифрация, алгоритм шифрования

# TECHNOLOGIES OF QUANTUM CRYPTOGRAPHY

***Evgeniy A. Dolgochub***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (913)932-07-05, e-mail: evgeniidolg@mail.ru

***Alexey N. Polikanin***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (913)397-63-51, e-mail: polikanin.an@yandex.ru

The article discusses the main classical algorithms of quantum cryptography, explaining the principle of operation of the mechanism for ensuring information security in the transmission of messages with the analysis of the polarization of photons. Conclusions are made about the most optimal variants of the combination of algorithms.

**Keywords:** quantum cryptography, decryption, encryption algorithm

## *Введение*

Криптография – это наука о методах предоставления неосуществимости чтения информации сторонним пользователем (конфиденциальность), неосуществимости изменения информации (целостность), проверки подлинности авторства или иных качеств предмета (аутентификация), а также неосуществимости отказа от авторства [1].

Перспектива квантовых компьютеров заключается в том, что некоторые вычислительные задачи могут выполняться экспоненциально быстрее на квантовом

процессоре, чем на классическом процессоре. Фундаментальная задача заключается в создании высокоточного процессора, способного выполнять квантовые алгоритмы в экспоненциально большом вычислительном пространстве.

В современном компьютерном мире способность шифровать сообщения необходима не только для того, чтобы держать некоторую информацию в секрете от других, но и является ключевой частью таких технологий, как криптовалюты, такие как биткойн. Кроме того, скандалы вокруг широко распространенного подслушивания разведывательных служб показали миру, что на самом деле ни одна из используемых сегодня процедур не является действительно безопасной. Но возможно, что через десять лет все коммуникации будут безопасными, потому что физически невозможно подслушать сообщения, зашифрованные квантовой криптографией.

## *Методы и материалы*

Текущее шифрование основано на алгоритме RSA [2] (названном в честь трех его изобретателей Ривеста, Шамира и Адлемана), который является «асимметричной» системой шифрования и использует комбинацию открытого ключа и закрытого ключа. Он основан на теории чисел, а алгоритм опирается на понятие простых чисел. Когда происходит процедура шифрования все, что ему нужно сделать, это просто умножить числа (что является очень простой задачей), заданные закрытым ключом и открытым ключом получателя. Получатель может расшифровать большое количество отправленных вами сообщений, используя их закрытый ключ и ваш открытый ключ.

Асимметрия возникает из-за сложности попытки расшифровать сообщение без знания закрытых ключей: получить большое число путем подслушивания процесса легко, но затем разложить большое число на два простых числа совершенно невозможно, если ключи достаточно длинные. Это потому, что факторизация очень большого числа на классическом компьютере заняла бы так много времени. Хотя не было строго доказано, что факторизация является «трудной проблемой» в математическом смысле, т.е. что не существует алгоритма, который решает его за полиномиальное компьютерное время, таких алгоритмов еще не найдено, и считается, что их не существует. На самом деле все известные классические алгоритмы занимают экспоненциально большое количество компьютерного времени.

Даже лучший классический алгоритм масштабируется экспоненциально с длиной ключа, в то время как алгоритм Шора может решить ту же проблему за полиномиальное компьютерное время. В то время как длинный ключ гарантирует, что текущие компьютеры не смогут взломать шифрование, это также означает, что RSA – это алгоритм, который не является математически безопасным, т. е. он мог бы быть взломан, если бы были доступны более крупные компьютеры. Этот тип безопасности иногда также называют вычислительно безопасным, т.е. если длина ключа выбрана достаточно большой, то даже суперкомпьютерам понадобятся сотни или тысячи лет, чтобы взломать сообщение.

Итак, выше мы только что установили, что классически даже лучшие алгоритмы для взлома шифрования RSA масштабируются экспоненциально со временем. Но в 1997 году произошел прорыв. Питер Шор показал в своей основополагающей статье, как можно разложить числа на множители за полиномиальное время на квантовом компьютере.

Большие квантовые компьютеры смогут взломать большинство существующих (классических) механизмов шифрования. Однако есть две причины, по которым пока не следует беспокоиться о раскрытии ключей шифрования.

С технологической точки зрения еще очень далеко до того момента, чтобы иметь квантовый компьютер, достаточно большой, чтобы разложить на множители любое серьезно большое число. Самое большое число, когда-либо факторизованное на квантовом компьютере, составляет сотни, что далеко от огромных чисел, необходимых для взлома RSA. Эквивалентной мерой мощности квантовых компьютеров является их количество кубитов (которые эквивалентны транзисторам классического компьютера). Современные квантовые компьютеры имеют несколько десятков кубитов, в то время как для правильной реализации алгоритма Шора потребовалось бы в тысячу раз больше.

Первая факторизация была выполнена на квантовом компьютере в 2001 году. [3] На самом деле алгоритм Шора является одним из самых сложных квантовых алгоритмов с точки зрения количества необходимых квантовых битов и элементов, и, по оценкам, пройдет несколько десятилетий, прежде чем будет выполнена какая-либо серьезная факторизация.

Несмотря на то, что это произойдет только в среднесрочной перспективе, алгоритм Шора представляет серьезную угрозу для всего, где важна секретность.

К счастью, для большинства ядов существует противоядие, и для алгоритма Шора оно называется: квантовая криптография. Но это не просто эволюционный шаг от современных методов криптографии, это не что иное, как революция, потому что это не только вычислительно безопасно, но и математически безопасно. Можно доказать, что подслушивающий никогда, даже с лучшим (квантовым или классическим) компьютером, не сможет взломать квантовое зашифрованное сообщение, потому что законы природы запрещают это делать.

Квантовая криптография математически безопасна, потому что законы природы запрещают подслушивать квантовое зашифрованное сообщение.

Самый прозрачный алгоритм квантовой криптографии также является первым найденным алгоритмом Беннетта и Брассарда, изобретенным в 1984 году [4, 5]. Он основан на одной из важнейших особенностей квантовой механики: возможности формирования суперпозиции между состояниями, например, между 0 и 1 квантового бита (кубита).

## *Результаты*

Алгоритм квантовой криптографии BB84.

Цель протокола состоит в том, что после выполнения Алиса и Боб оба используют один и тот же ключ, с помощью которого они могут шифровать сообщения с невозможностью доступа к ним третьего лица.

Протокол работает следующим образом: Алиса создает множество кубитов (например, одиночные фотоны) и готовит каждый из них в случайном состоянии, где она не только выбирает «0» или «1», но готовит она «0» или «1» в z-базисе или x-базисе. Физически «z-базис» или «x-базис» в случае фотонов означают, что она либо использует линейно поляризованный свет, либо циркулярно поляризованный свет, а «0» и «1» означают горизонтальный (или вертикальный) или поворот вправо (или влево). Подготовив эти кубиты, она отправляет их Бобу.

Один из способов реализации первых двух шагов алгоритма: Алиса готовит одиночные фотоны и отправляет их Бобу. Фотоны готовятся в одном из четырех состояний: свет с круговой поляризацией справа или слева или свет с горизонтальной/вертикальной линейной поляризацией.

Затем Боб измеряет каждый кубит в случайно выбранном базисе. Это, в частности, означает, что он может измерять в «неправильном» базисе, то есть не в том, в котором Алиса подготовила кубит.

После Боб объявляет, на каком базисе он измерил кубиты, а Алиса говорит, правильно ли он измерил. Если он измеряет в правильном базисе, это означает, что Алиса и Боб теперь делятся знаниями о результатах измерения. Например, если Алиса подготовила «1» в z-базисе, а Боб измеряет в z-базисе, то он получит «1», и они могут использовать эту «1» в качестве цифры своего ключа. Если бы он, однако, измерял в x-базисе, у него был бы 50% - ный шанс получить неправильный результат измерения. Например, Алиса могла бы подготовить кубит «0» в x-базисе, который является равной суперпозицией «0» и «1» в z-базисе. Когда Боб измеряет в z-базисе, у него, следовательно, есть 50 % шанс измерить «0» и 50 % шанс измерить «1» – это означает, что Алиса и Боб не могут использовать этот кубит для своего ключа, потому что в 50 % всех случаев у них не будет одного и того же числа.

Они могут использовать в качестве ключа все числа, измеренные в правильном базисе. Но если Ева перехватит передачу и измерит кубиты, прежде чем отправить их Бобу, она сможет изменить результаты измерений Боба.

Поэтому, на части кубитов, измеренных в правильном базисе (например, на половине из них), Боб объявляет результаты своих измерений, а Алиса – значения, с которыми она их подготовила. Если теперь они обнаружат, что некоторые значения не совпадают, они могут заподозрить, что Ева пыталась перехватить их. Это потому, что она может делать только то же самое, что и Боб: измерять на случайном базисе. Если теперь она измеряла в «неправильном» базисе, а Боб – в «правильном», может случиться так, что Алиса и Боб не согласятся с результатом измерения.

Пример для BB84: Алиса готовит 10 кубитов случайным образом и отправляет их Бобу. Боб измеряет в случайном базисе, получая некоторые результаты, после чего они оба транслируют свою базу и обсуждают их, уничтожая кубиты, которые были измерены Бобом в неправильном базисе. На половине кубитов, которые в порядке, они также обсуждают результаты измерения. Если они получают совпадающие результаты, они принимают результаты измерений в качестве своего ключа, который состоит из оставшихся неубранных кубитов.

## *Обсуждение*

Основа квантовой безопасности: квантовая информация не может быть скопирована.

Этот удивительный факт, известный под названием «теорема об отсутствии клонирования», был обнаружен только через 70 лет после появления квантовой механики несмотря на то, что он был доказан буквально в двух строках расчетов [6]. Также довольно интересна история его открытия: это произошло во время рецензирования статьи, которая пыталась доказать что-то физически невозможное. Несмотря на то, что это противоречило некоторым из самых фундаментальных понятий физики, рецензентам было трудно показать, где была ошибка. В конце концов они обнаружили теорему об отсутствии клонирования, которая опровергла сообщение.

И из-за невозможности клонирования информации квантовая криптография физически защищена от подслушивающих устройств, т. е. за исключением технических несовершенств из-за шума, ее невозможно взломать.

## *Заключение*

Штат Женева в Швейцарии уже использует квантовую криптографию на выборах в течение десяти лет. Основываясь на алгоритме BB84 машины, поставляемые швейцарским стартапом Idquantique, сочетают традиционную криптографию RSA с действительно случайным ключом, созданным квантовым распределением ключей.

Совсем недавно важный шаг на пути к глобальной сети безопасной квантовой связи был сделан благодаря внедрению спутникового распределения квантовых ключей китайской исследовательской группой вокруг Цзянь Вэй-Пана. Это был один из первых плодов, собранных в рамках масштабной программы квантовых технологий китайского правительства на сумму 10 миллиардов долларов [11].

Эта демонстрация была не только встречена одобрительными возгласами в западном мире, даже названа «моментом спутника» квантовых технологий, поскольку она показала, что Китай на много миль опережает достижение действительно безопасной связи. Вскоре после этого Европа инициировала свой «квантовый флагман» стоимостью 1 млрд евро с помощью «квантового манифеста», и даже администрация Трампа объявила, что они запустят в стране «Национальную квантовую инициативу» стоимостью 10 млрд долларов. Это всего лишь вопрос нескольких лет, когда квантовая связь и другие квантовые технологии будут использоваться в устройствах потребительского уровня.

Квантовые процессоры, основанные на сверхпроводящих кубитах, могут выполнять вычисления в гильбертовом пространстве размером $253 \times 9 \times 1015$, недоступном для самых быстрых классических суперкомпьютеров, доступных сегодня. Насколько известно, этот эксперимент знаменует собой первое вычисление, которое может быть выполнено только на квантовом процессоре [7].

С приходом на свободный рынок квантовых компьютеров традиционная криптография устареет. Связано это с вычислительной мощностью, которая теоретически в квадрат раз [10] превосходит стандартные компьютеры за счет исчисления информации не в битах, а в кубитах.

Выводы:

1) защита лишь на физическом уровне не может дать полноценной конфиденциальности;

2) совмещение квантовых алгоритмов шифрования с математическими может дать устойчивый к атакам метод шифрования.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Алферов, А.П. Основы криптографии : учебное пособие / Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. – Москва : Гелиос АРВ, 2001.– 479 с.

2. Бауэр, Ф. Расшифрованные секреты. Методы и принципы криптологии [Текст] /Бауэр Ф. – Москва: Мир, 2007.– 550 с.

3. Бунин, О. Занимательное шифрование [Электронный ресурс] : журнал / отдел «Мир ПК». – Электрон. дан. – 2003.– Режим доступа: https://www.osp.ru/pcworld/2003/07/166048. – Загл. с экрана.

4. Головашич, С. А. Анализ эффективности проектирования алгоритмов участников конкурса БСШ Украины [Электронный ресурс] : статья /отдел «Методика оценки алгоритмов блочного симметричного шифрования» – XI Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». – Электрон. дан. – Киев, 2008.– 31 с.

5. Головашич, С. А. Анализ эффективности проектирования алгоритмов-участников конкурса БСШ Украины : отчет / Головашич С. А. – Харьков : ООО «КРИПТОМАШ», 2009.– 70 с.

6. Дошина, А. Д. Криптография. Основные методы и проблемы. Современные тенденции криптографии / Михайлова А. Е., Карлова В. В./ Современные тенденции технических наук: материалы IV Междунар. науч. конф. – Казань: Бук, 2015.— С. 10-13.

7. Кузнецов, А. А. Разработка предложений по совершенствованию симметричных средств защиты информации перспективной системы критического применения. /А. А. Кузнецов, И. В. Москвиченко. – Харьков. – 2008. – С. 94 – 100.

8. Lieven M. K. et al. Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance// Nature 414. 20–27 Dec. 2001. – pp. 883–887.

9. Nechvatal J. Report on the Development of the Advanced Encryption Standard (AES). / J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, - Journal of Research of the National Institute of Standards and Technology, Volume 106, Number 3, May–June 2001. – pp. 511–577.

10. Румянцев К. Е., Плёнкин А. П., Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищенности. // Радиотехника. . — 2015. — № 2. — С. 125—134.

11. Susan Decker, Christopher Yasiejko, Forget the Trade War. China Wants to Win the Computing Arms Race. Bloomberg, apr 09, 2018 [Electronic resource]. – Mode of access: https://www.industryweek.com/technology-and-iiot/article/22025445/forget-the-trade-war-china-wants-to-win-the-computing-arms-race (дата обращения: 17.06.2021).