УДК 535.14
DOI: 10.33764/2618-981X-2020-6-1-125-130

АНАЛИЗ КВАНТОВЫХ АЛГОРИТМОВ ШИФРОВАНИЯ BB84 И B92

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. (383)343-91-11, e-mail: polikanin.an@yandex.ru

Канал связи, защищённый квантовой криптографией в идеальных условиях невозможно взломать. Но только потому, что на данный момент не существует подходящих методов взлома. Все существующие методы взлома криптографических сетей направлены на математические модели шифров. Однако, если следовать правилу, что стойкость системы определяется стойкостью её самого слабого звена, то мы можем убедиться в обратном. Квантовая криптография является перспективным молодым и развивающимся направлением в области защити информации. Каждый специалист в сфере информационной безопасности заинтересован в создании совершенной и защищенной сети связи. Системы, которые на данный момент используют протокола BB84 и B92 подвержены атакам со стороны злоумышленников. Данные протоколы защиты уже считаются устаревшими, однако учёные пока не могут предложить других вариантов. В статье рассматриваются преимущества и недостатки квантовых алгоритмов шифрования BB84 и B92, которые являются первыми алгоритмами квантового шифрования.

Ключевые слова: криптография, квантовые методы шифрования, поведение квантов, квантовая физика, поляризация, фотоны.

ANALYSIS OF QUANTUM BB84 AND B92 ENCRYPTION ALGORITHMS

Evgeny A. Dolgochub
Siberian state University of geosystems and technologies, 10 Plahotnogo 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 Plahotnogo st., Novosibirsk, 630108, Russia, senior lecturer, Department of information security, phone: (383)343-91-11, e-mail: polikanin.an@yandex.ru

A communication channel protected by quantum cryptography cannot be hacked under ideal conditions. But only because there are currently no suitable hacking methods available. All existing methods of breaking cryptographic networks are aimed at mathematical models of ciphers. However, if we follow the rule that the stability of a system is determined by the stability of its weakest link, we can see the opposite. Quantum cryptography is a promising young and developing field in the field of information security. Every specialist in the field of information security is interested in creating a perfect and secure communication network. Systems that currently use the BB84 and B92 protocols are vulnerable to attacks from hackers. These security protocols are already considered

outdated, but scientists can not yet offer other options. The article discusses the advantages and disadvantages of the first quantum encryption algorithms BB84 and B92.

Key words: cryptography, quantum encryption methods, quantum behavior, quantum physics, polarization, photons.

Введение

Квантовая криптография – это метод защиты информации, основанный на принципах квантовой физики, рассматривает случаи переноса информации с помощью объектов квантовой механики. Данный метод защиты считается одним из самых надежных в теории методов [1]. Многие современные институты проводят исследования, но до глобального использования данного метода защиты еще пока далеко. Используемая в квантовой криптографии аппаратура является очень сложной и дорогостоящей [2]. Ниже представлена принципиальная схема квантового канала связи (рис. 1).

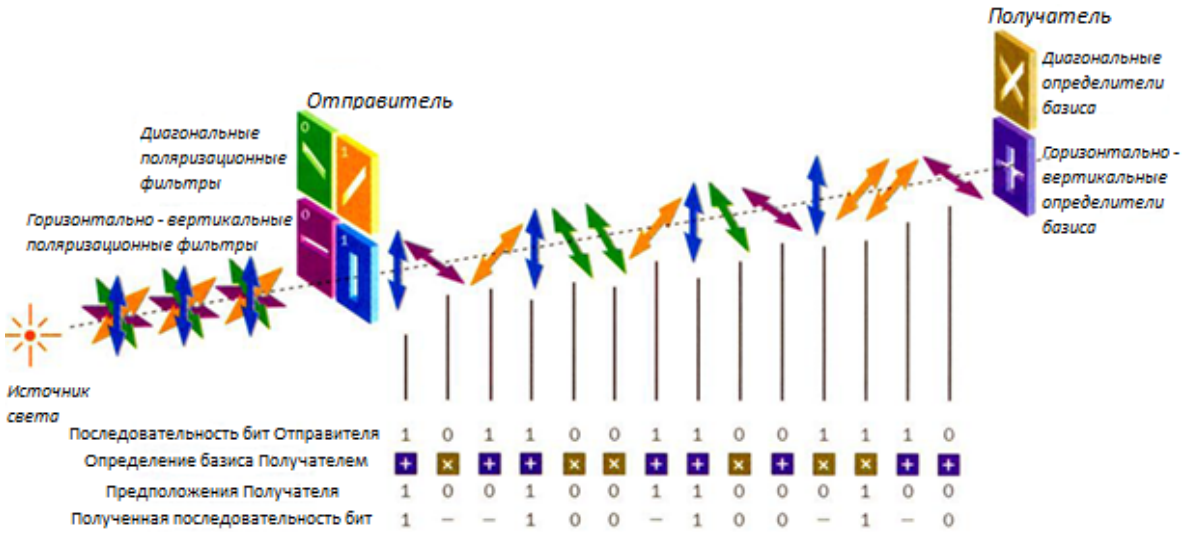

Рис. 1. Принципиальная схема квантового канала связи «(рисунок получен из открытого интернет-источника <https://www.pvsm.ru/budushhee/324062>)»

Технология квантового распределения криптографических ключей решает одну из основных задач криптографии — гарантированное на уровне фундаментальных законов природы распределение ключей между удаленными пользователями по открытым каналам связи. Криптографический ключ — это числовая последовательность определенной длины, созданная для шифрования информации [3]. Квантовая криптография позволяет обеспечить постоянную и автоматическую смену ключей при передаче каждого сообщения в режиме одноразового «шифроблокнота»: на сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью. Ключевой особенностью такой системы является то, что любые атаки, любые попытки подслушивать будут немедленно обнаружены.

Принципы алгоритма BB84

Впервые идея шифрования информации с помощью квантовых объектов появилась в 1970 году. Первая схема защиты информации была предложена в 1984 году. Алгоритм назвали «BB84». Суть алгоритма заключается в возможности легальных пользователей обмениваться сообщениями, представленными в виде поляризованных фотонов по квантовому каналу под углами 0, 45, 90 и 135 градусов.

Протокол использует четыре квантовых состояния, образующих два базиса. Состояния внутри одного базиса – ортогональны, но состояния из разных базисов неортогональны. Такая особенность позволяет определить попытки несанкционированного доступа к информации. Информация представлена поляризованными под четырьмя разными углами фотонами. С помощью измерения можно различить только два состояния:

– фотон поляризован вертикально или горизонтально;

– фотон поляризован под углами 45 или 135 градусов.

Достоверно за одно измерение отличить горизонтальный фотон от фотона, поляризованного под углом 135 градусов невозможно.

Пример связи по методу «BB84» представлен ниже.

1) Отправитель случайно выбирает один из базисов. Затем случайным образом выбирает одно из состояний и посылает фотоны (табл. 1);

Таблица 1

Возможные состояния

Обозначение	Поляризация	Бит
↔	Под углом 90	1
↕	Под углом 180	0
↗	По углом 45	0
↖	По углом 135	1

2) Получатель случайным образом и независимо выбирает для каждого поступающего фотона прямолинейный или диагональный базис и измеряет в нем значение фотона (табл. 2);

Таблица 2

Обозначения анализаторов

Обозначение	Поляризация
+	Прямоугольный
×	Диагональный

3) Для каждого переданного состояния получатель по открытому каналу связи сообщает базис, в котором проводилось измерение, но результаты измерений остаются в секрете;

4) Отправитель открыто сообщает получателю, какие измерения были выбраны;

5) Пользователи канала связи оставляют только те случаи, в которых выбранные базисы совпали. Эти случаи переводят в биты и составляют ключ (табл. 3).

Таблица 3

Конечное представление

Последовательность фотонов отправителя	↕	↗	↗	↔	↖	↕	↕	↔	↔
Последовательность анализаторов получателя	+	×	+	+	×	×	×	+	×
Результаты измерений получателя	0	0	1	1	1	0	1	1	0
Выбор анализаторов	+	+	-	+	+	-	-	+	-
Ключ	0	0		1	1			1	

Примерно 50 % данных теряется. Если имело место прослушивание канала, то по величине ошибки можно оценить максимальное количество информации, доступное злоумышленнику. Существует оценка, что если ошибка на канале меньше 11 %, то секретная передача данных по каналу возможна, так как информация, доступная злоумышленнику заведомо не превосходит информацию между получателем и отправителем [4]. Такая информация называется взаимной. Взаимная информация вычисляется по формуле:

$$I_{AB}(D) = \frac{1}{2}\varphi(1-2D), \tag{1}$$

где $I_{AB}(D)$ – взаимная информация; φ – количество использованных базисов; D – доля ошибок в канале (в относительных единицах).

Взаимная информация между отправителем и злоумышленником равна:

$$I_{AE}(D) = \frac{1}{2} + \frac{x}{2}\left(\frac{1}{2} - \sqrt{2D - 4D^2}\right) + \frac{x}{2}\left(\frac{1}{2} + \sqrt{2D - 4D^2}\right), \tag{2}$$

где x – количество информации в битах.

Для случая равновероятного использования двух базисов:

$$I_{AE}(D) = \frac{1}{2}\varphi\left(2\sqrt{D(1-D)}\right). \tag{3}$$

На данный протокол существует два метода атак:

– атака для случая однофотонных сигналов;

– атака разделения числа фотонов.

Для атаки в случае однофотонных сигналов подразумевается, что все передаваемые сигналы содержат строго один фотон [5]. Атаки разделяются на коге-

рентные и некогерентные. При когерентном классе атак злоумышленник любым способом перепутывает пробу любой размерности с целой группой передаваемых фотонов. При некогерентном классе злоумышленник перехватывает фотоны, измеряет их состояние и затем отправляет их получателю [6].

Так как в настоящее время однофотонные источники не созданы, используются слабокогерентные импульсы. Вероятность содержания в импульсе n фотонов определяется распределением Пуассона:

$$P_{n.loss} = e^{-\eta\mu} \frac{(\eta\mu)^n}{n!}, \quad (4)$$

где $P_{n.loss}$ – вероятность содержания в импульсе n фотонов μ – среднее число фотонов в импульсе; η - коэффициент передачи канала.

Если злоумышленник обнаруживает в импульсе более одного фотона, он отводит один, остальные беспрепятственно доходят до получателя. Затем злоумышленник перепутывает перехваченный фотон со своей пробой и ожидает объявления базисов. Следовательно, он получит точное значение переданного бита, не внося при этом никаких ошибок.

История развития и принципы алгоритма B92

Протокол B92 был предложен в 1992 году. Он основан на принципе неопределенности, носителями информации будут являться двух уровневые системы (кубиты). Важной особенностью данного метода является использование двух неортогональных состояний [7]. Данный протокол является модификацией протокола BB84. В качестве базиса используются следующие поляризации:

1) линейная
   - горизонтальная;
   - вертикальная;
2) круговая
   - правая круговая;
   - левая круговая.

Исходя из принципа неопределённости Гейзенберга нельзя при измерении достоверно отличить два неортогональных состояния кванта, а соответственно определение значения бита будет невозможно, а любые попытки определить состояние кубита непредсказуемо его изменят [8]. Данный протокол проще в реализации из–за использования всего двух состояний для кодирования, однако получить надлежащую надежность при таком протоколе является очень сложной задачей. Протокол может оказаться совсем небезопасным [9].

Вывод

Распределение ключей зависит от определенной модификации алгоритма, однако протокол B92 не стал конкурентом BB84. Существенных изменений в алгоритме не произошло, но вычислить злоумышленника стало сложнее потому, что теперь он может внести лишь 12,5 % ошибок в ключ. В протоколе BB84 вно-

силось 25 % [10]. Полезными для генерации ключа остается лишь четверть фотонов. 75 % данных просто теряется. Существование большого ряда трудностей в практической реализации, огромные потери данных и дороговизна постановки системы на потоковое производство также дают отрицательную оценку этого протокола. Преимущество дает лишь необходимость использования двух источников для реализации протокола B92 вместо четырех. Низкая скорость генерации фотонов, срабатывающие на лишние частицы датчики и оптические потери в современных оптоволоконных линиях связи не дают возможности применить алгоритм B92.

Подводя итоги, можно сделать следующие выводы:

– любые квантовые протоколы требуют оригинального дорогостоящего оборудования;

– ни один квантовый протокол не может обходиться без дополнительного классического канала связи;

– для всех квантовых протоколов существуют проблемы доказательства корректности и реализация протокола на персональных компьютерах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Квантовая криптография / шифрование [Электронный ресурс]. – Режим доступа : http://www.tadviser.ru/index.php/Статья:Квантовая_криптография_%28шифрование%29 (дата обращения: 07.04.2020).

2. Lieven M. K. Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance// Nature 414. 20–27 Dec. 2001 (дата обращения: 09.04.2020).

3. Классическая криптография [Электронный ресурс]. – Режим доступа : https://en.ppt-online.org/13814 (дата обращения: 07.04.2020).

4. Preneel B. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. / B. Preneel, A. Biryukov, C. De Canni`ere1, S. B. Ors, E. Oswald, B. Van Rompay1, - Berlin, Springer-Verlag, April 19, 2004 - Version 0.15 (beta) (дата обращения: 09.04.2020).

5. Lieven M. K. Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance// Nature 414. 20–27 Dec. 2001 (дата обращения: 08.04.2020).

6. Experimental quantum cryptography [Electronic resource]. – Mode of access : https://link.springer.com/article/10.1007%2FBF00191318 (дата обращения: 03.04.2020).

7. Повышение скорости шифрования в кватернионных криптосистемах, Кузнецова К.С., Духнич Е.И. [Электронный ресурс]. – Режим доступа : https://elibrary.ru/item.asp?id=32351753 (дата обращения: 09.04.2020).

8. Квантовый компьютер и криптографическая стойкость современных систем шифрования [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/kvantovyy-kompyuter-i-kriptograficheskaya-stoykost-sovremennyh-sistem-shifrovaniya (дата обращения: 07.04.2020).

9. Nechvatal J. Report on the Developmentof the Advanced Encryption Standard (AES). / J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, - Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, October 2, 2000 (дата обращения: 03.04.2020).

10. Криптографические системы [Электронный ресурс]. – Режим доступа : https://mynet-notes.livejournal.com/2437.html (дата обращения: 07.04.2020).