УДК 003.26 + 004.056.55 Вестник УрФО № 4(26) / 2017, с. 25–27

Филиппов М. А., Кротова Е. Л.

КВАНТОВАЯ КРИПТОГРАФИЯ. ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Статья посвящена квантовой криптографии, её отличиям от традиционной криптографии. Особое внимание авторы уделяют преимуществам и недостаткам квантовой криптографии и её актуальности в современном мире. За последние три десятилетия криптография с открытым ключом стала неотъемлемым компонентом нашей глобальной цифровой инфраструктуры связи. Эти сети поддерживают множество приложений, которые важны для нашей экономики, нашей безопасности и нашего образа жизни, таких как мобильные телефоны, интернет-коммерция, социальные сети и облачные вычисления. В таком связанном мире способность людей, предприятий и правительств безопасно общаться, имеет первостепенное значение.

Ключевые слова: *Криптография, квантовая криптография, шифрование.*

Filippov M.A., Krotova E.L.

QUANTUM CRYPTOGRAPHY. ADVANTAGES AND DISADVANTAGES

The article is devoted to quantum cryptography, its differences from traditional cryptography. Special attention is paid to the advantages and disadvantages of quantum cryptography and its relevance in the modern world. Over the past three decades, public-key cryptography has become an integral component of our global digital communications infrastructure. These networks support many applications that are important to our economy, our security and our way of life, such as mobile phones, e-commerce, social networks and cloud computing. In such a connected world, the ability of people, businesses and governments to communicate securely is of paramount importance.

Keywords: *cryptography, quantum cryptography, encryption.*

Многие из наших наиболее важных коммуникационных протоколов основаны главным образом на трех основных криптографических функциях: шифрование с открытым ключом, цифровые подписи и обмен ключами. В настоящее время эти функции в основном реализуются с использованием обмена ключами Диффи-Хеллмана, криптосистемы RSA и криптосистемы эллиптической кривой. Их безопасность зависит от сложности определенных теоретико-числовых задач, таких как факторизация целых чисел или проблема дискретного журнала для разных групп. В скором времени начнут появляться квантовые компьютеры, новые технологии, использующие физические свойства материи и энергии для выполнения расчетов, которые смогут эффективно решать каждую из этих проблем, тем самым делая все криптосистемы с открытым ключом на основе таких допущений бесполезными в области защиты. Таким образом, достаточно мощный квантовый компьютер будет представлять угрозы безопасности многим формам современной коммуникации - от обмена ключами до шифрования и цифровой аутентификации. Долгое время методы разработки алгоритмов шифрования определялись только хитростью и изо-

бретательностью их создателей. И только в XX веке данной областью заинтересовались математики, а потом — и физики, что и привело к появлению квантовой криптографии[1].

Что такое квантовая криптография и её отличие от обычной криптографии

Классическая криптография решает фактически только две задачи: защиту передаваемых сообщений от прочтения и от модификации сторонними лицами. Она базируется на использование симметричных алгоритмов шифрования, в которых зашифровывание и расшифрование различаются лишь порядком исполнения и направлением некоторых простых шагов. Эти методы используют один и тот же скрытый элемент (ключ), и второе действие (расшифрование) является простым обращением первого (зашифрования). Поэтому любой из участников обмена может как зашифровать, так и расшифровать сообщение. По причине большой избыточности естественных языков непосредственно в зашифрованное сообщение очень тяжело внести осмысленное изменение, поэтому классическая криптография гарантирует также защиту от навязывания ложных данных. Если же естественной избыточности оказывается недостаточно для надежной защиты сообщения от модификации, она может быть искусственно увеличена методом добавления к нему особой контрольной комбинации. Если сказать вкратце, то защищённость классической криптографии строиться на уверенности в том, что злоумышленник не успеет за разумное время «взломать» шифр ввиду сложности используемых алгоритмов[2].

Квантовая криптография — способ защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические способы, чтобы обеспечить секретность информации, квантовая криптография сконцентрирована на физике, изучая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации постоянно выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определённых параметров физических объектов — в нашем случае, переносчиков информации. Обобщённо можно сказать, что защищённость квантовой криптографии выстраивается на утверждении о том, что никто не сможет «взломать» шифр, так как это противоречит физическим законам природы.

Преимущества и недостатки квантовой криптографии

К преимуществам квантовой криптографии можно отнести:

– Обнаружение пассивного перехватчика – атака злоумышленника вносит значительно больше ошибок, чем их возникает в квантовом канале в результате естественного шума.

– Теоретико-информационная стойкость распределения ключей – ключи, распределённые с помощью квантовых протоколов с теоретико-информационной стойкостью, используется для дальнейшего шифрования с использованием известных классических симметричных алгоритмов. Поэтому общий уровень стойкости криптосистемы повышается.

– Защищённость основана на фундаментальных физических законах и принципах.

– Однако также существуют недостатки:

– Не является полноценным завершённым решением защиты информации – необходима предварительная аутентификация пользователей; пользователи не имеющие никакого общего предустановленного начального секрета, не могут обменяться новым ключом для шифрования.

– С увеличением длины квантового канала значительно уменьшается скорость передачи – если длина канала >100 км, то скорость передачи составляет биты в секунду, хотя на расстояниях в 20-30 км уже достигают мегабитных скоростей.

– Деполяризация фотонов в квантовом канале приводит к достаточно высокому уровню естественных помех.

– Сложность реализации и высокая стоимость оборудования приводит к сильной конкуренции на рынке средств защиты информации, что в свою очередь заканчивается банкротством для небольших компаний3.

Заключение

Подводя итог, хотелось бы сказать, что последние разработки в области квантовой криптографии позволяют формировать системы, обеспечивающие фактически 100%-ю защиту ключа и информации. Используя знания по защите информации, как из классиче-

ской криптографии, так и из новейшей «квантовой» области, люди смогут получать результаты, превосходящие все известные криптографические системы4. Сегодняшняя квантовая криптография разработана с прицелом на будущее, в котором взлом классических шифров с открытым ключом может стать практически достижимым. Например, однажды квантовый компьютер сможет взломать сегодняшние шифры. Квантовая криптография также представляет собой прекрасный пример тесного взаимодействия между фундаментальными и прикладными исследованиями.

Литература:

1. Lily Chen Stephen Jordan Yi-Kai Liu Dustin Moody Rene Peralta Ray Perlner Daniel Smith-Tone "Report on Post-Quantum Cryptography", NISTIR 8105 DRAFT Phys. Rev. A, Vol. 15, 2016

2. Классическая и «современная» криптография. // Как устроен блочный шифр? URL: http://www.enlight.ru/crypto/articles/vino-kurov/blcyph_1.htm (дата обращения 09.06.2017)

3. Современные технологии квантовой защиты информации // DOCPLAYER. URL: http://docplayer.ru/38223070-Sovremennye-tehnologii-kvantovoy-zashchity-informacii.html (дата обращения 12.06.2017)

4. Квантовая криптография. // VIII Международная студенческая электронная научная конференция «Студенческий научный форму» - 2016 URL: https://www.scienceforum.ru/2016/1543/17525 (дата обращения 15.06.2017)

References

1. Lily Chen Stephen Jordan Yi-Kai Liu Dustin Moody Rene Peralta Ray Perlner Daniel Smith-Tone "Report on Post-Quantum Cryptography", NISTIR 8105 DRAFT Phys. Rev. A, Vol. 15, 2016.

2. Klassicheskaya i «sovremennaya» kriptografiya. // Kak ustroyen blochnyy shifr? URL: http://www.enlight.ru/crypto/articles/vino-kurov/blcyph_1.htm (data obrashcheniya 09.06.2017).

3. Sovremennyye tekhnologii kvantovoy zashchity informatsii // DOCPLAYER. URL: http://docplayer.ru/38223070-Sovremennye-tehnologii-kvantovoy-zashchity-informacii.html (data obrashcheniya 12.06.2017).

4. Kvantovaya kriptografiya. // VIII Mezhdunarodnaya studencheskaya elektronnaya nauchnaya konferentsiya «Studencheskiy nauchnyy formu» - 2016 URL: https://www.scienceforum.ru/2016/1543/17525 (data obrashcheniya 15.06.2017)

ФИЛИППОВ Михаил Александрович, студент кафедры Автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: Misha-Fill@mail.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра Высшей математики Пермского национального исследовательского политехнического университета, доцент. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

FILIPPOV Mikhail, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 614990, Permsky Kray, Perm, Komsomolsky Prospekt, 29. E-mail: Misha-Fill@mail.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 614990, Permsky Kray, Perm, Komsomolsky prospekt, 29. E-mail: lenkakrotova@yandex.ru