Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Кондрашева П.П. Что такое квантовая криптография? // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2018. – №12 (декабрь). – АРТ 609-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

УДК 3937

Кондрашева Полина Павловна

студентка 2 курса, факультет информационных систем и технологий

Научный руководитель: Глущенко А.Г., заведующий кафедрой физики, доктор физико-математических наук, профессор

ФГБОУ ВПО «Поволжский государственный университет телекоммуникаций и информатики»

г. Самара, Российская Федерация

e-mail: polya.kondrashewa@yandex.ru

ЧТО ТАКОЕ КВАНТОВАЯ КРИПТОГРАФИЯ?

Аннотация: В статье рассмотрено понятие о квантовой криптографии. Затронута также тема о новых разработках в данной области.

Ключевые слова: квантовая криптография, защита, коммуникация, фотон.

Kondrashewa Polina

2nd year student, features of information systems and technology

Supervisor: Glushchenko, A.G, Head of the Department of Physics, Doctor of Physics and Mathematics, Professor

FGBOU VPO "Povolzhskiy State University telecommunications and informatics"

Samara, Russian Federation

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

WHAT IS QUANTUM CRYPTOGRAPHY?

Abstract: The article discusses the concept of quantum cryptography.
Keywords: quantum cryptography, protection, communication, photon.

Квантовая криптография — это способ защиты коммуникаций, который сформулирован на принципах квантовой физики. В отличие от классической криптографии, которая применяет математические способы, чтобы сохранить секретность данной информации, квантовая криптография сконцентрирована на физике информации, потому что учитывает случаи, когда информация распространяется с помощью объектов квантовой механики. Процесс отправки и получение информации всегда осуществляется физическими средствами, например, при помощи электронов в электрическом токе.

Это направление достаточно новое, но медленно развивающиеся в силу своей нестандартности и трудности. С научной точки зрения это не есть криптография в понимании данного слова, потому что строиться она не столько на математических типах, сколько на физики квантовых частиц. Самой главной её отличительной чертой, а заодно и спецификой любой квантовой структуры является невозможность вскрытия состояния конструкции на протяжении времени, так при первом же измерении структуры меняет свое состояние на одно из возможных неортогональных значений. Кроме всего прочего есть «Теорема о запрете клонирования», сформулированная в 1982 году Вуттерсом, Зуреком и Диэксом, она говорит о недопустимости создания идеальной копии произвольного неизвестного квантового состояния, однако есть способ, а именно — создание неточной копии. Для этого нужно привести начальную систему в взаимосвязь с

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

большей вспомогательной системой и провести унитарное изменение общей структуры, в результате которого несколько составляющих второй структуры станут почти копиями исходной.

Также хотелось бы затронуть тему экспериментальных реализаций и перейти к примерам. 13 декабря 2017 года компания ИнфоТеКС информировала о представлении «Квантового телефона ViPNet» – системы, демо-продукт был создан в лаборатории квантовых оптических технологий физического факультета МГУ, и VPN ViPNet (на примере двух других систем – ViPNet Client и ViPNet Connector). Квантовый телефон ViPNet разрешает соединять рабочие станции с установленным ПО ViPNet и кодировать трафик между ними с применением квантового распределения ключей. Квантовое распределение ключей позволяет предоставить надежный уровень безопасности при передаче данных по открытым каналам связи, способствует ликвидации угрозы вычисления ключей защиты на квантовых компьютерах, а также как стало известно 30 августа 2017 года, ученые из университета Оттавы успешно провели первые реальные испытания технологии квантового 4D-кодирования, передав зашифрованные сообщения между двумя станциями, которые были расположены на крышах высотных зданий, расстояние между которыми составляло 300 метров.

Классические технологии квантовых коммуникаций, уже используемые в некоторых местах для создания "невзламываемых" квантовых сетей, используют стандартную двоичную систему счисления, которая кодирует в одном фотоне один бит передаваемой информации. Некоторое время назад была изобретена технология многомерного квантового кодирования, которая разрешает увеличить объем информации в 2 раза, заключенной в одном фотоне света. Это позволяет каждому фотону

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

нести одно из четырех значений — 00, 01, 10 и 11, вследствие чего данная технология получила название квантового 4D-кодирования. Помимо того, технологию отличает более надежный уровень защиты от попыток преднамеренного вмешательства и высокая устойчивость к влиянию посторонних факторов окружающей среды.

Теперь можно и перейти к выводу, что применение идей квантовой механики уже открыло новую эпоху в этой области, так как способы квантовой криптографии открывают новые возможности в этой сфере передачи сообщений, которые даже теоретически нельзя «расшифровать», и работы над коммерческими системами такого рода уже идут полным ходом.

Список использованной литературы:

1. Квантовая криптография: идеи и практика / под ред. С.Я.Килина, Д.Б.Хорошко, А.П.Низовцева. – Мн., 2008. – 392 с.
2. Kilin S.Ya. Quanta and information / Progress in optics. – 2001. – Vol. 42. – P. 1–90.
3. Килин С. Я. Квантовая информация / Успехи Физических Наук. – 1999. – Т. 169. – С. 507-527.
4. Васильев М.Н., Горшков *А.В.*Разработка и создание аппаратно-программного комплекса для автоматизированного томографического анализа пучков заряженных частиц с высоким пространственным разрешением. / Аннотированный НТО по программе "Управляемый термоядерный синтез и плазменные процессы." - Долгопрудный: МФТИ, 01.12.1992. - 30 с.

Дата поступления в редакцию: 20.12.2018 г.
Опубликовано: 26.12.2018 г.