Гаджиев Г.К. Развитие технологий квантовой криптографии и их роль в обеспечении информационной безопасности // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 10(48) с. 34–37

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

РАЗВИТИЕ ТЕХНОЛОГИЙ КВАНТОВОЙ КРИПТОГРАФИИ И ИХ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гаджиев Г.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: gugac134@gmail.com

Введение квантовой криптографии представляет собой революционное направление в области информационной безопасности, особенно актуальное в свете развития квантовых компьютеров и растущих вычислительных угроз. Квантовая криптография, основываясь на принципах квантовой механики, предлагает непревзойденные уровни защиты данных за счет использования квантовых свойств частиц. В статье рассматриваются ключевые принципы квантовой криптографии, включая принцип неделимости квантового состояния, квантовую телепортацию и квантовое шифрование. Основные преимущества квантовой криптографии, такие как абсолютная безопасность, невозможность подслушивания и высокая скорость передачи данных, обсуждаются наряду с вызовами, включая техническую сложность и ограничения на расстояние передачи. Перспективы применения квантовой криптографии обширны и охватывают защиту критической инфраструктуры, медицинских данных, финансовых транзакций и облачных вычислений. Статья подчеркивает, что несмотря на существующие вызовы, квантовая криптография имеет потенциал стать фундаментом будущих систем информационной безопасности, обеспечивая надежную защиту данных в цифровом мире.

Ключевые слова: Квантовая криптография, информационная безопасность, квантовые компьютеры, квантовая телепортация, квантовое шифрование.

DEVELOPMENT OF QUANTUM CRYPTOGRAPHY TECHNOLOGIES AND THEIR ROLE IN ENSURING INFORMATION SECURITY

Gadzhiev G.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The introduction of quantum cryptography represents a revolutionary direction in the field of information security, especially relevant in light of the development of quantum computers and growing computing threats. Quantum cryptography, based on the principles of quantum mechanics, offers unmatched levels of data security by exploiting the quantum properties of particles. The article discusses the key principles of quantum cryptography, including the principle of indivisibility of a quantum state, quantum teleportation and quantum encryption. The main advantages of quantum cryptography, such as absolute security, the impossibility of eavesdropping, and high data transfer rates, are discussed along with the challenges, including technical complexity and limitations on transmission distance. The application prospects for quantum cryptography are broad and span the protection of critical infrastructure, medical data, financial transactions and cloud computing. The article emphasizes that despite existing challenges, quantum cryptography has the potential to become the foundation of future information security systems, providing reliable data protection in the digital world.

Keywords: Quantum cryptography, information security, quantum computers, quantum teleportation, quantum encryption.

Введение

С развитием цифровых технологий и распространением интернета возросла значимость вопросов информационной безопасности. Современные методы шифрования, основанные на классической криптографии, сталкиваются с угрозами со стороны вычислительных атак и развития квантовых компьютеров. В этой связи разработка и применение квантовой криптографии становится все более актуальной задачей.

Основные принципы квантовой криптографии

Квантовая криптография основана на использовании квантовых свойств физических объектов, таких как фотоны, для обмена и защиты информации. Основные принципы квантовой криптографии включают:

Согласно этому принципу, нельзя скопировать или измерить квантовое состояние без его разрушения. Это обеспечивает безопасность передачи информации, так как любая попытка перехвата или прослушивания сигнала приведет к изменению его состояния и обнаружению подслушивателя.[1]

Этот принцип позволяет передавать информацию между двумя точками без физической передачи частиц. Вместо этого используется перенос квантового состояния между двумя удаленными точками, что обеспечивает безопасную передачу информации.

Этот принцип заключается в использовании квантовых свойств для создания криптографических ключей и шифрования данных. Это позволяет создавать абсолютно безопасные системы шифрования, которые невозможно взломать с помощью классических методов.

Квантовая криптография обладает рядом преимуществ, которые делают ее привлекательной для применения в системах информационной безопасности:

Использование принципов квантовой механики обеспечивает абсолютную безопасность передачи информации. Даже с учетом развития квантовых компьютеров, методы квантовой криптографии остаются устойчивыми к вычислительным атакам.

Принцип неделимости квантового состояния и принцип квантовой телепортации обеспечивают невозможность подслушивания при передаче информации, что делает квантовую криптографию идеальным инструментом для защиты конфиденциальных данных.[2]

Квантовая криптография позволяет передавать данные с очень высокой скоростью, что делает ее эффективной для использования в сетях высокоскоростной передачи данных.

Несмотря на многочисленные преимущества, у квантовой криптографии есть и некоторые недостатки и вызовы, которые следует учитывать:

Внедрение квантовой криптографии требует высокотехнологичного оборудования и специализированных знаний, что может быть сложно и затратно для многих организаций.

Квантовая телепортация и передача квантовых состояний ограничены расстоянием, что может ограничивать применение квантовой криптографии в глобальных сетях.

Для успешного внедрения квантовой криптографии необходимо интегрировать ее с существующими системами информационной безопасности, что может потребовать значительных усилий и времени.

Несмотря на вызовы и недостатки, квантовая криптография обладает большим потенциалом и широкими перспективами применения в обеспечении информационной безопасности:[3]

Применение квантовой криптографии может привести к развитию квантовых сетей, которые будут обеспечивать абсолютную безопасность передачи информации между узлами сети.

Квантовая криптография может быть использована для защиты критической инфраструктуры, такой как системы управления энергоснабжением и транспортные сети, от кибератак и кибершпионажа.[4]

В сфере здравоохранения квантовая криптография может обеспечить безопасную передачу медицинских данных и личной информации пациентов, что критически важно для обеспечения конфиденциальности и целостности этих данных.

В финансовом секторе квантовая криптография может использоваться для защиты финансовых транзакций и данных клиентов от киберпреступников и мошенников.

Квантовая криптография может улучшить безопасность облачных вычислений, защищая данные, хранимые и передаваемые через облачные сервисы, от утечек и атак.

Заключение

Квантовая криптография представляет собой инновационную и перспективную область в обеспечении информационной безопасности. Основываясь на принципах квантовой механики, она предлагает уникальные преимущества, такие как абсолютная безопасность передачи данных и невозможность их подслушивания. [5] Однако внедрение квантовой криптографии сопряжено с рядом технических и организационных вызовов, включая необходимость сложного оборудования, ограничения на расстояние передачи данных и интеграцию с существующими системами. Несмотря на эти вызовы, потенциал квантовой криптографии в различных областях — от защиты критической инфраструктуры и медицинских данных до финансовых транзакций и облачных вычислений — делает её важным инструментом для будущего цифровой безопасности. Развитие квантовых сетей и дальнейшее совершенствование квантовых технологий обещают значительно усилить защиту информации и способствовать созданию новых, более безопасных систем связи. С учетом продолжающегося прогресса в данной области, квантовая криптография имеет все шансы стать ключевым элементом обеспечения безопасности в цифровом мире.

Список литературы

1. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности //Известия высших учебных заведений. Технология легкой промышленности. – 2017. – Т. 37. – №. 3. – С. 5-9.
2. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом //СПб.: СПбГУТ. – 2014. – Т. 176.
3. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии //Телекоммуникации. – 2020. – №. 8. – С. 14-20.
4. Березина Е. О., Виткова Л. А., Ахрамеева К. А. Классификация угроз информационной безопасности в сетях IOT //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 11-18.
5. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.

References

1. Tsvetkova L. A., Vakhrameeva K. A., Gruzinsky B. A. The use of geometric hash functions in information security //News of higher educational institutions. Light industry technology. - 2017. – Vol. 37. – No. 3. – pp. 5-9.
2. Nechaeva K. A. Development of undetectable stegosystems for channels with noise //St. Petersburg: SPbSUT. – 2014. – Vol. 176.
3. Akhrameeva K. A. et al. Analysis of the means of exchanging hidden data by intruders on the Internet using steganography methods //Telecommunications. - 2020. – No. 8. – pp. 14-20.
4. Berezina E. O., Tsvetkova L. A., Vakhrameeva K. A. Classification of information security threats in IT networks //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 11-18.

5. Virrich E. V., Ferapontova S. S. On the issue of personal data audit //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – pp. 111-114.