УДК 004.056

Галимова А.Р., Домрачева В.Е.,
Шарафутдинов Б.И., Ямилова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

ОСОБЕННОСТИ КВАНТОВЫХ МЕТОДОВ КРИПТОГРАФИИ: ПРИНЦИПЫ, РЕАЛИЗАЦИЯ И ПЕРСПЕКТИВЫ

Аннотация. В статье рассматриваются особенности квантовой криптографии и протокола BB84, а также их отличие от традиционных методов. Анализируются принципы квантовой механики, лежащие в основе распределения ключей (КРК), такие как принцип Гейзенберга и квантовая суперпозиция. Описаны существующие системы КРК, их плюсы и минусы. Обсуждаются перспективы развития квантовой криптографии и ее роль в защите информации будущего.

Ключевые слова: квантовая криптография, квантовое распределение ключей (КРК), протокол BB84, квантовая суперпозиция, принцип неопределенности, кубиты, безопасность информации.

В условиях усиления угроз кибербезопасности, обусловленных развитием вычислительной техники, в том числе квантовых компьютеров, традиционные криптографические методы становятся все более уязвимыми. Квантовая криптография, использующая законы квантовой механики для защиты передаваемой информации [1]. Основным направлением является квантовое распределение ключей (КРК), позволяющее двум сторонам установить общий секретный ключ, устойчивый к перехвату [2–4]. КРК основывается на двух принципах квантовой механики: квантовой суперпозиции: кубит (наименьшая единица в информации) может одновременно представлять значения 0 и 1, описывается вектором состояния

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ где } |\alpha|^2 + |\beta|^2 = 1,$$

и принципе неопределенности Гейзенберга. Измерение кубита изменяет его состояние, что позволяет обнаружить любые попытки взлома сообщения.

Протокол BB84. Протокол квантового распределения ключей в котором используется для кодирования информации четыре квантовых состояния двухуровневой системы, формирующие два сопряженных базиса. Носителями информации являются 2-уровневые системы, называемые кубитами (квантовыми битами). Протокол включает следующие этапы:

– подготовка и передача кубитов: например, Алиса генерирует случайные биты, кодирует их в кубиты с использованием двух базисов и отправляет Бобу;

– измерение кубитов: например, Боб измеряет кубиты, выбирая один из базисов;

– объявление базисов: например, Алиса и Боб обмениваются информацией о использованных базисах, сохраняя только согласованные биты;

– оценка ошибок: например, Алиса и Боб сравнивают часть согласованных битов для выявления ошибок;

– исправление ошибок: например, если уровень ошибок приемлем, применяются протоколы исправления.

– усиление приватности: например, Алиса и Боб используют методы для получения абсолютно секретного ключа.

Рассмотрим далее основные методы реализации протокола КРК.

Существуют разные реализации КРК систем, каждая из которых имеет свои плюсы и минусы:

– волоконно-оптические системы: передают фотоны по оптическому волокну, но ограничены расстоянием из-за потерь;

– спутниковые системы: используют спутники для передачи на большие расстояния, нуждаются в специальном оборудовании и подвержены атмосферным влияниям;

– системы свободного пространства: передают фотоны с помощью лазерных лучей в атмосфере, требуют прямой видимости и также подвержены влиянию погоды.

Рассмотрим далее основные преимущества и недостатки методов квантовой криптографии. Преимущества этого метода:

– высокий уровень защиты передаваемых сообщений: КРК гарантирует безопасность, опираясь на фундаментальные принципы физики, а не на вычислительную сложность математических алгоритмов;

– устойчивость к взлому алгоритмов: QKD не зависит от криптографических алгоритмов, потенциально уязвимых в будущем.

Основные недостатки метода:

– ограничения дистанции передачи сообщений: потери в квантовой среде ограничивают дальность передачи ключей, что требует применения квантовых ретрансляторов;

– техническая сложность реализации: развертывание КРК-систем требует использования специализированного и дорогостоящего оборудования;

– совместимость: КРК-системы требуют специальной инфраструктуры и не совместимы с существующими классическими сетями связи.

Квантовая криптография обладает значительным потенциалом для защиты информации. Ожидается дальнейшее развитие QKD-систем,

включая увеличение дальности, скорости генерации ключей и снижение стоимости. Она может защитить важные объекты инфраструктуры, банковские системы и государственные сети.

Квантовая криптография – это революционный подход к информационной безопасности, основанный на квантовой механике. Протокол BB84 лежит в основе современных QKD-систем. Несмотря на ограничения, квантовая криптография может сыграть важную роль в защите информации, особенно в условиях угроз со стороны квантовых компьютеров.

Список использованных источников:

1. Bennett C.H., & Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. P. 175–179.

2. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dušek M., Lütkenhaus N., & Peev, M., 2009. The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.

3. Gisin N., Ribordy, G., Tittel, W., & Zbinden H. Quantum cryptography. Reviews of Modern Physics, 2002, 74 (1), 145.

4. Lütkenhaus N. (2018). Quantum key distribution. Nature Physics, × 14 × (12), 1168–1170. URL: https://arxiv.org/pdf/1905.09197v2.

Domracheva V.E., Galimova A.R.,
Sharafutdinov B.I., Iamilova A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

FEATURES OF QUANTUM CRYPTOGRAPHY METHODS: PRINCIPLES, IMPLEMENTATION, AND PROSPECTS

Abstract. The article discusses the features of quantum cryptography and the BB84 protocol, as well as their differences from traditional methods. The principles of quantum mechanics underlying key distribution (QKD), such as the Heisenberg principle and quantum superposition, are analyzed. The existing QKD systems, their pros and cons are described. The prospects for the development of quantum cryptography and its role in protecting the information of the future are discussed.

Keywords: quantum cryptography, quantum key distribution (QKD), BB84 protocol, quantum superposition, uncertainty principle, qubits, information security.