УДК 621.396

Максимова София Михайловна

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ КВАНТОВЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Технологические достижения, достигнутые в последнее время, особенно в области искусственного интеллекта (ИИ) и квантовых вычислений, привели к значительным изменениям в технологиях. Эти достижения оказали глубокое влияние на квантовую криптографию, область, в которой методологии искусственного интеллекта обладают огромным потенциалом для повышения эффективности и надежности криптографических систем. Однако появление квантовых компьютеров создало новую проблему для существующих алгоритмов безопасности, обычно называемую 'квантовой угрозой'. Несмотря на эти

проблемы, существуют многообещающие пути интеграции искусственного интеллекта на основе нейронных сетей в криптографию, что имеет значительные последствия для будущих парадигм цифровой безопасности. В этом резюме освещаются ключевые темы пересечения искусственного интеллекта и квантовой криптографии, включая потенциальные преимущества криптографии на основе искусственного интеллекта, проблемы, которые необходимо решить, и перспективы этой междисциплинарной области исследований.

Квантовые компьютеры, криптография, кубиты, квантовое распределение ключей, искусственный интеллект.

Maximova Sofia Mikhailovna

RESEARCH ON THE APPLICATION OF QUANTUM ENCRYPTION ALGORITHMS TO ENSURE CYBERSECURITY

Recent technological advances, especially in the fields of artificial intelligence (AI) and quantum computing, have led to significant changes in technology. These advances have had a profound impact on quantum cryptography, an area in which artificial intelligence methodologies have enormous potential to improve the efficiency and reliability of cryptographic systems. However, the advent of quantum computers has created a new problem for existing security algorithms, commonly referred to as the 'quantum threat'. Despite these challenges, there are promising ways to integrate artificial intelligence based on neural networks into cryptography, which has significant implications for future digital security paradigms. This summary highlights the key topics of the intersection of artificial intelligence and quantum cryptography, including the potential benefits of artificial intelligence-based cryptography, the challenges that need to be addressed, and the prospects for this interdisciplinary field of research.

Quantum computers, cryptography, qubits, quantum key distribution, artificial intelligence.

Введение

В последние годы технологии развивались с огромной скоростью, что привело к радикальным изменениям в вычислительной технике. Квантовые вычисления, в частности, привлекли внимание своей способностью революционизировать наши представления о вычислительной мощности и эффективности [2]. Они используют принципы квантовой механики для выполнения вычислений с беспрецедентной скоростью и точностью по сравнению с традиционными компьютерами.

Квантовые компьютеры имеют огромный потенциал, и их возможности применения практически безграничны. Они обсуждаются наряду с другими передовыми технологиями, такими как искусственный интеллект и машинное обучение, в современном цифровом мире. Применяемые технологии реализуют принципы квантовой физики и механики, включая основные её параметры: квантовую запутанность и принцип суперпозиции. Эти параметры используются компьютером для работы с данными, что для обычных компьютеров невозможно.

Главная цель использования квантовых компьютеров – работа с кубитами – основными единицами хранения информации в подобных системах.

Это повысило бы потенциал квантовых компьютеров и позволило бы выполнять более сложные вычисления [1]. Крупные технологические корпорации вкладывают значительные средства в эту область, чтобы преодолеть это препятствие.

Основная часть

Квантовая криптография — это передовая область, использующая принципы квантовой механики, для обеспечения беспрецедентного уровня конфиденциальности связи. В отличие от традиционных методов шифрования, которые зависят от сложных математических задач, квантовая криптография использует внутреннюю нестабильность квантовых частиц, что делает попытки взлома практически неосуществимыми [9].

Квантовые компьютеры приближаются к вычислительной мощности и стабильности, необходимой для взлома протоколов шифрования с открытым ключом, что делает переход на постквантовую криптографию необходимым. Постквантовая криптография использует законы квантовой физики для передачи личных данных не обнаруживаемым способом, что называется квантовым распределением ключей. Такой подход к криптографии нацелен на распределение ключей между пользователями по обычному каналу связи.

Квантовая криптография использует принципы квантовой механики для создания не поддающихся взлому ключей шифрования. Она кодирует данные с помощью фотонов для обеспечения безопасной передачи между сторонами. Поляризация и рандомизация состояний фотонов повышают безопасность данных, а теорема квантового клонирования обеспечивает конфиденциальность данных [10].

Криптографический ключ — это последовательность чисел определенной длины, которая используется для шифрования данных [4]. Кванто-

вые криптографические протоколы гарантируют, что ключ меняется динамически и автоматически при каждом обмене сообщениями с использованием одноразовой клавиатуры, которая является наиболее безопасной формой шифрования, доступной в настоящее время. Данные протоколы шифрования необходимы для защиты коммуникаций, финансовых транзакций и конфиденциальной личной информации. Однако с появлением квантовых вычислений возникли опасения по поводу эффективности существующих методов шифрования.

Перспективная технология квантового распределения ключей (QKD) использует квантовую механику для безопасного шифрования, передачи и дешифрования данных. Системы QKD используют квантовую механику для обнаружения любых попыток несанкционированного доступа, обеспечивая тем самым конфиденциальность сообщений. Этот инновационный подход способен произвести революцию в защите данных, обеспечив беспрецедентный уровень безопасности для современного мира, управляемого цифровыми технологиями.

Технология квантового шифрования основана на кодировании информации в квантовых состояниях, таких как поляризация фотонов. Эти частицы функционируют как крошечные защищенные контейнеры, содержащие секретные данные, к которым невозможно получить доступ без непосредственного взаимодействия с ними. Квантовые системы обладают отличительной особенностью: любая попытка отслеживать или перехватывать квантовое состояние неизбежно приводит к его разрушению. Следовательно, злоумышленник не может подслушать или скопировать информацию, не оставив следов, которые предполагаемый получатель немедленно обнаружил бы.

Современные алгоритмы открытых ключей используются для аутентификации, цифровой подписи, шифрования данных и ввода ключей в действие [4]. Однако, квантовые компьютеры представляют потенциальную угрозу безопасности, так как они могут быть использованы для взлома этих алгоритмов [8]. По результатам проведенных исследований, в США создали список инструкций, в которых описываются возможные результаты применения квантовых компьютеров и их угрозы для безопасности, которые возникнут при создании и использовании кардинально новых подходов к шифрованию и взлому криптографической защиты.

Из всех существующих алгоритмов наибольшую устойчивость к потенциальному взлому с использованием квантового компьютера показал

алгоритмы AEC и SHA255, но только при том условии, если заданная длина ключа будет превышать стандартные параметры не менее чем в 3 раза. Подобные блочные шифры останутся актуальны и некоторое время смогут противостоять системам взлома, основанных на использовании квантовых компьютеров.

BB84 – один из самых известных протоколов в области квантовой криптографии, и его безопасность была доказана множеством исследований [5]. С практической точки зрения, квантовая криптография может быть уязвима для атак с помощью неотключаемых физических функций и LPA (атаки на основе света). Однако протоколы SARG04 (защита от удаленных атак) и trap-state повышают надежность распределения ключей и увеличивают расстояние передачи для квантового распределения ключей.

Квантовая запутанность проявляется в том, что две или более частицы становятся взаимосвязанными, сохраняя эту связь даже на огромных расстояниях. Это явление обеспечивает беспрецедентный уровень безопасности при передаче данных. Любая попытка перехватить или подслушать информацию неизбежно разрушит запутанность, сигнализируя о несанкционированном доступе.

Для противостояния угрозам, связанных с квантовыми вычислениями существуют два основных подхода: квантовое распределение (КРК) и постквантовая криптография (ПК). Квантовое распределение ключей эксплуатирует свойства квантовых частиц, делая невозможным перехват или копирование информации без её разрушения. Сгенерированные ключи устойчивы к атакам всех видов и находят применение в исследовательских центрах и государственных организациях для защиты конфиденциальных данных. Постквантовая криптография фокусируется на создании математических задач, устойчивых ко взлому с помощью квантовых компьютеров. Эти алгоритмы не поддаются взлому ни сейчас, ни в будущем.

КРК и ПК подходят к конкретным ситуациям: в первом случае это защита государственных данных, а во втором защита конфиденциальной информации как сейчас, так и в будущем. Сравнение методов отражено в табл. 1.

Таблица 1

Сравнение методов криптографии

Метод	Преимущества	Недостатки
Асимметричная криптография	Легко реализовать, широко используется	Уязвима к атакам квантовых компьютеров
Квантовое распределение ключей	Обеспечивает абсолютную безопасность	Требует специализированного оборудования, ограниченная дальность действия
Постквантовая криптография	Устойчива к квантовым атакам	Находится на ранней стадии разработки, стандарты еще не приняты

Выбор метода защиты данных зависит от конкретных требований и доступных ресурсов:

– асимметричная криптография: подходит для не конфиденциальных данных или ситуаций, где не требуется абсолютная безопасность;

– квантовое распределение ключей: используется для защиты конфиденциальных данных, требующих максимального уровня безопасности;

– постквантовая криптография: перспективный метод, но его внедрение потребует времени и стандартизации.

Для обеспечения безопасной передачи данных устройство может быть оснащено модулями квантовой криптографии. Однако широкому внедрению этой технологии препятствует отсутствие надежной инфраструктуры квантовых сетей. Передача квантовых частиц на большие расстояния сопряжена с техническими трудностями, требующими разработки каналов, устойчивых к помехам.

Криптография, основанная на квантовых принципах, имеет как значительные преимущества, так и недостатки. КК требует сложного специализированного оборудования и высококвалифицированного персонала для установки и обслуживания систем [7]. Также возникают сложности с передачей достоверной информации на большие расстояния, поскольку требует использовать ретрансляторы. Всё это сильно повышает стоимость требуемого оборудования для обеспечения работоспособности систем.

Квантовые частицы обладают свойствами суперпозиции, одновременно являясь логическим нулём и единицей. Связь между ними гарантирует целостность информации, так как при изменении состояния одного – мгновенно изменяется и другой элемент. На текущее время в какой-то степени

реализованы два метода: BB84, использующий поляризацию фотонов, и E91, использующий квантовую запутанность [2]. Отправитель создает пары запутанных частиц, отправляя одну частицу получателю, а другую сохраняя для собственного использования. После измерения поляризации обе стороны получают случайную последовательность.

Выводы

В России активно ведутся разработки в области квантовой криптографии, направленные на создание надежных и защищенных систем связи. Основными направлениями являются квантовые криптографические системы на базе атмосферной оптики, использующие атмосферный канал для передачи квантовых сигналов, что позволяет реализовать связь на большие расстояния, например, между наземными станциями или космическими аппаратами; квантовые интерфейсы, позволяющие сопрягать квантовые устройства с классическими каналами связи; квантовые ретрансляторы необходимые для увеличения дальности передачи информации и построения разветвленных сетей; квантовая память, позволяющая хранить квантовые состояния в течение длительного времени, что имеет важное значение для обеспечения надежной работы квантовых сетей. Развитие квантовой криптографии в России осуществляется в рамках национальной программы по созданию квантовой инфраструктуры. Эта программа объединяет усилия научных учреждений, университетов и компаний.

Квантовая криптография идеально подходит для защиты секретной информации, передаваемой по каналам связи, будь то военные секреты, государственные документы или конфиденциальные сведения топменеджмента [6]. Она может использоваться для защиты систем управления и контроля на объектах критической инфраструктуры, таких как электростанции, транспортные системы и системы связи и обеспечивать должный уровень защиты информации, которая хранится длительное время [4].

Квантовые протоколы могут быть использованы для обеспечения нового уровня анонимности и конфиденциальности передаваемой информации при онлайн-коммуникации, что имеет крайне важное значение в современном цифровом мире. Однако, несмотря на значительный потенциал, квантовая криптография все еще находится на достаточно ранних стадиях разработки [3].

Недавно был разработан новый алгоритм для обнаружения возможных угроз квантовым генераторам случайных чисел, что еще больше повышает безопасность этих систем. Квантовые вычисления потенциально

могут повлиять на асимметричное шифрование, которое зависит от сложного математического процесса, включая разложение больших чисел на простые множители. Если квантовые компьютеры получат широкое распространение, долгосрочная жизнеспособность традиционных методов шифрования может быть поставлена под угрозу.

Квантовая не является заменой традиционным методам шифрования, а дополняет их, предлагая более высокий уровень безопасности для наиболее чувствительных данных. Традиционные методы шифрования, такие как шифрование с открытым ключом и симметричное шифрование, имеют свои преимущества, такие как простота реализации, низкая стоимость и широкое распространение. Однако, они также имеют недостатки, такие как уязвимость к квантовым компьютерам и риск утечки ключей. Квантовая криптография, с другой стороны, обеспечивает абсолютную безопасность, гарантирует целостность данных и подходит для защиты конфиденциальных данных. Но имеет свои ограничения, такие как сложность реализации, ограниченная дальность действия и высокая стоимость.

БИБЛИГРАФИЧЕСКИЙ СПИСОК

1. Квантовый компьютер: что это, как работает и на что способен // Skillbox Media – URL: https://skillbox.ru/media/code/chto-takoe-kvantovyy-kompyuter-i-kak-on-rabotaet/

2. Что такое шифрование? | Шифрование данных | Определение шифрования // Kaspersky.ru – URL: https://www.kaspersky.ru/resource-center/definitions/encryption.

3. *Штеренберг С.И., Бударный Г.С., Ахметов Р.Р.* Обеспечение безопасности криптографии в условиях квантовых вычислений// Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 585-586.

4. *Гельфанд А.М., Сигачева В.В., Архипов А.В., Сиротина Л.К.* Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры // Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 21-27.

5. *Гоулд Р., & Беннет С.* (2016). Применение квантовой криптографии для безопасной передачи данных. Журнал криптографии и информационной безопасности, 12(4), 215-230.

6. Batch fully homomorphic encryption over the integers / J.H. Cheon [et al.] // Advances in Cryptology – EUROCRYPT'2013 (LNCS). – 2013. – Vol. 7881. – P. 315–335

7. *Заргарян Е.В., Морозов Н.В.* Необходимость разработки системы обнаружения утечек на нефтепроводе/ В сборнике: Донецкие чтения 2023: образование, наука, инновации, культура и вызовы современности. Материалы VIII Международной научной конференции. Донецк, 2023. С. 141-143.

8. *Заргарян Е.В., Рой Ю.В.* Сепарация газа на промыслах и типы применяемых устройств. В сборнике: Технологии разработки информационных систем ТРИС-2020. Материалы X Международной научно-технической конференции. "Технологии разработки информационных систем", 2020. С. 143-149

9. *Ганциевский А.В., Заргарян Е.В.* Анализ существующих методов оптической сепарации ТБО/ Молодёжный вестник Новороссийского филиала Белгородского государственного технологического университета им. В.Г. Шухова. 2023. Т.3. №2 (10). С. 188-191.

10. *Заргарян Е.В., Филонова Е.С.* Эффекты применения технологий IIOT в системах интеллектуального управления освещением на производстве// В сборнике: Прикладные вопросы точных наук. Материалы VII Международной научно – практической конференции студентов, аспирантов, преподавателей. 2023. С. 121 – 124.

Максимова София Михайловна, студентка Политехнического института (филиал) ДГТУ в г. Таганроге, Россия, город Таганрог, улица Петровская 109а, 347904, телефон: +7 (928) 778-71-94, email: sofiamaksimova.2003@mail.ru.

Maximova Sofia Mikhailovna, student of the Polytechnic Institute (branch) of DSTU in Taganrog, Russia, Taganrog, Petrovskaya street 109a, 347904, phone: +7 (928) 778-71-94, email: sofiamaksimova.2003@mail.ru.