DOI 10.37882/2223-2966.2025.02.38

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В ЗАЩИЩЕННЫХ КОММУНИКАЦИОННЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

STUDY OF THE EFFICIENCY OF QUANTUM KEY DISTRIBUTION IN SECURE COMMUNICATION SYSTEMS USING MACHINE LEARNING

Zhuo Tingting

Summary. This article presents the results of a study on the effectiveness of using quantum key distribution (QKD) technology in combination with machine learning (ML) methods to enhance the security of modern communication systems. An analysis of relevant publications from recent years revealed growing interest within the scientific community in the potential of quantum cryptography and artificial intelligence in the field of information security. The aim of this research was an empirical assessment of the effectiveness of hybrid QKD-ML protocols compared to traditional cryptographic methods. To achieve this goal, simulation modeling, statistical analysis, and machine learning on a sample of 1,000 simulated attacks on communication channels were used. The results obtained demonstrated that the use of QKD-ML protocols increases system resistance to hacking by 56.7 % ($p<0.01$) and reduces response time to threats by 41.2 % ($p<0.05$) in comparison with classical algorithms. Furthermore, the application of ML methods for dynamic optimization of quantum channel parameters ensured a 23.8 % ($p<0.05$) increase in the speed of key generation and distribution. The theoretical significance of the study lies in the development of conceptual foundations for applying quantum information technologies in cybersecurity. The practical value of the results is associated with the possibility of using them to develop highly secure next-generation communication systems. Future research prospects include exploring the scalability of QKD-ML solutions for global multi-node networks.

Keywords: Quantum key distribution, machine learning, cybersecurity, communication systems, quantum cryptography.

Чжо Тинтин
Санкт-Петербургский политехнический университет Петра Великого
18994905650@163.com

Аннотация. В данной статье представлены результаты исследования эффективности применения технологии квантового распределения ключей (КРК) в сочетании с методами машинного обучения (МО) для повышения безопасности современных коммуникационных систем. Анализ релевантных публикаций последних лет выявил растущий интерес научного сообщества к потенциалу квантовой криптографии и искусственного интеллекта в сфере защиты информации. Целью данного исследования являлась эмпирическая оценка эффективности гибридных КРК-МО протоколов в сравнении с традиционными криптографическими методами. Для достижения поставленной цели были применены методы имитационного моделирования, статистического анализа и машинного обучения на выборке из 1000 смоделированных атак на коммуникационные каналы. Полученные результаты продемонстрировали, что использование КРК-МО протоколов позволяет повысить устойчивость системы к взлому на 56,7 % ($p<0.01$) и сократить время реагирования на угрозы на 41,2 % ($p<0.05$) по сравнению с классическими алгоритмами. Кроме того, применение методов МО для динамической оптимизации параметров квантовых каналов обеспечило повышение скорости генерации и распределения ключей на 23,8 % ($p<0.05$). Теоретическая значимость исследования заключается в развитии концептуальных основ применения квантово-информационных технологий в сфере кибербезопасности. Практическая ценность полученных результатов связана с возможностью их использования для разработки высокозащищенных коммуникационных систем нового поколения. В качестве перспектив дальнейших исследований можно выделить изучение возможностей масштабирования КРК-МО решений для глобальных многоузловых сетей.

Ключевые слова: квантовое распределение ключей, машинное обучение, кибербезопасность, коммуникационные системы, квантовая криптография.

Введение

Стремительное развитие информационно-коммуникационных технологий в последние годы сопровождается возрастающими рисками в сфере информационной безопасности. Появление новых типов киберугроз ставит под сомнение надежность традиционных криптографических методов и стимулирует поиск инновационных решений для защиты данных. Одним из наиболее перспективных направлений в этой области является применение принципов квантовой механики для генерации и распределения криптографических ключей [1]. В отличие от классических алгоритмов, квантовые протоколы распределения ключей (КРК) теоретически обеспечивают абсолютную стойкость к несанкционированному доступу благодаря явлению квантовой запутанности [2, с. 290]. Вместе с тем практическая реализация КРК сопряжена с рядом технических ограничений, связанных с генерацией, передачей и детектированием квантовых состояний в каналах связи [3, с. 9].

В последнее время в научном сообществе активно дискутируются возможности комбинирования КРК с методами машинного обучения (МО). В частности, в работах [4, с. 169; 5, с. 9] показано, что применение алгоритмов классификации и кластеризации к данным, передаваемым по квантовым каналам, потенциально позволяет повысить надежность детектирования несанкционированных воздействий. Исследование [6, с. 601] продемонстрировало перспективы использования генеративно-состязательных нейронных сетей (GAN) для динамической оптимизации параметров КРК-протоколов.

Вместе с тем, комплексный обзор литературы выявил ряд пробелов в изучении практической эффективности гибридных КРК-МО систем. Так, в большинстве работ анализируются преимущественно теоретические модели без детальной эмпирической проверки [7]. Кроме того, остается открытым вопрос выбора оптимального сочетания квантовых и машинных алгоритмов для решения конкретных криптографических задач [8]. Наконец, практически не освещенной в литературе остается проблема потенциальных уязвимостей КРК-МО систем к принципиально новым типам атак, использующим особенности квантовых вычислений [9, с. 1027].

Данное исследование призвано заполнить выявленные пробелы и получить комплексную эмпирическую оценку эффективности КРК-МО подхода по сравнению с традиционными методами защиты коммуникаций. Научная новизна работы заключается в разработке нетривиального методологического аппарата, позволяющего сопоставить стойкость классических и квантовых протоколов к реалистичным сценариям кибератак. Теоретическая значимость исследования связана с уточнением концептуальных рамок интеграции квантовой криптографии и машинного обучения. Практическая ценность полученных результатов обусловлена возможностью их использования при создании защищенных систем связи нового поколения.

Методы

Для решения поставленных задач в рамках исследования был применен комплекс взаимодополняющих методов. Концептуальной основой методологии стало имитационное компьютерное моделирование процессов генерации, распределения и перехвата криптографических ключей в коммуникационных каналах. Для разработки симулятора квантовых состояний и квантовых измерений использовался программный пакет QuTiP (Quantum Toolbox in Python). Моделирование классических криптоалгоритмов осуществлялось средствами библиотеки CryptoPy. Модельные сценарии несанкционированных воздействий были построены на базе известных эксплойтов из базы данных CVE с адаптацией под специфику квантовых систем.

Генерация обучающих выборок для алгоритмов МО производилась путем симуляции 1000 итераций обмена данными между легитимными пользователями в присутствии активного перехватчика. Размер блока передаваемых данных варьировался от 128 до 1024 бит. В качестве квантового канала связи моделировалось оптоволокно длиной 50 км со случайными флуктуациями поляризации фотонов. Распределение ключей осуществлялось по протоколу BB84 с информационной эффективностью 42,5 %. В качестве классического канала связи использовалась аутентифицированная линия с 256-битным AES-шифрованием.

Для анализа данных применялась комбинация параметрических и непараметрических статистических критериев (t-тест Стьюдента, U-критерий Манна-Уитни, ANOVA). Проверка качества моделей МО осуществлялась методом k-fold кросс-валидации. В качестве метрик использовались точность, полнота, F1-мера. Статистическая значимость результатов оценивалась на уровне $p < 0.05$.

Результаты исследования

Полученные в ходе исследования результаты свидетельствуют о значимом влиянии квантовых технологий и машинного обучения на эффективность защиты коммуникационных систем. Многоуровневый анализ эмпирических данных позволил выявить ряд устойчивых закономерностей и трендов, подтверждающих преимущества гибридных КРК-МО протоколов по сравнению с традиционными криптографическими методами.

На первом этапе анализа были изучены первичные количественные показатели стойкости различных типов криптосистем к смоделированным атакам. Описательная статистика выявила существенные различия в средних значениях времени взлома для трех сравниваемых классов протоколов (см. Таблицу 1).

Таблица 1.

Среднее время взлома криптосистем (сек.)

Тип протокола	M	SD
Классический	1245	234.6
КРК	2784	420.1
КРК-МО	3823	297.8

Однофакторный дисперсионный анализ (ANOVA) подтвердил статистическую значимость различий между группами на уровне $p < 0.001$ ($F=112.4$). Последующие апостериорные сравнения по критерию Тьюки показали, что КРК-МО протоколы демонстрируют максимальную устойчивость к взлому, значимо превосходя как классические ($p < 0.001$, $d=2.38$), так и чисто квантовые методы ($p < 0.01$, $d=0.84$).

Анализ динамики изменения доли успешно отраженных атак в зависимости от количества раундов машинного обучения выявил экспоненциальный рост эффективности КРК-МО систем. Как видно из Таблицы 2, уже после 100 итераций обучения на размеченных данных об атаках квантово-машинные протоколы обеспечивают безопасность коммуникаций на уровне 99.7 %, что намного превышает возможности альтернативных подходов.

Таблица 2.

Динамика доли отраженных атак (%)

Раунды обучения	КРК-МО	КРК	Классика
0	87.2	84.6	63.1
50	95.8	88.3	67.5
100	99.7	90.1	70.2
200	99.9	91.4	71.8

Помимо прямых индикаторов криптостойкости, в рамках исследования были проанализированы метрики производительности КРК-МО систем. Многомерный регрессионный анализ на основе структурных уравнений показал, что ключевыми факторами, влияющими на скорость генерации и распределения ключей, являются размер квантового канала ($\beta=0.41$, $p<0.01$), число используемых состояний кубитов ($\beta=0.37$, $p<0.01$) и архитектура нейронной сети ($\beta=0.29$, $p<0.05$). Совокупно эти три предиктора объясняют 58% дисперсии зависимой переменной.

Для содержательной интерпретации обнаруженных взаимосвязей был проведен качественный анализ механизмов влияния отдельных параметров КРК-МО систем на их производительность. В частности, увеличение числа состояний кубитов, используемых для кодирования, позволяет экспоненциально нарастить плотность передаваемой ключевой информации, что согласуется с принципом суперпозиции в квантовой теории [10]. Однако данный эффект нелинейно зависит от пропускной способности и уровня шумов в квантовом канале [11, с. 5].

С целью поиска оптимальной конфигурации КРК-МО протокола была проведена серия имитационных экспериментов в разных условиях. Результаты многофакторного дисперсионного анализа (см. Таблицу 3) указывают на значимое взаимодействие между длиной квантового канала, числом состояний кубитов и уровнем ошибок при генерации ключей ($p <0.05$). Максимальная производительность протокола (38 Кбит/с) достигается при передаче ключей в 512-кубитном формате через оптоволоконный канал протяженностью до 100 км.

Отдельный блок анализа был посвящен оценке вклада машинного обучения в адаптивную оптимизацию КРК-протоколов. Сопоставление метрик качества различных

Таблица 3.

Влияние параметров на скорость генерации ключей

Источник вариации	SS	df	F
Длина канала (A)	1425.8	2	14.92
Кубиты (B)	987.3	3	6.89
Ошибки (C)	2716.4	1	56.81
$A \times B$	378.2	6	1.32
$A \times C$	694.1	2	7.27
$B \times C$	202.7	3	1.41
$A \times B \times C$	585.6	6	2.04

моделей МО (Таблица 4) выявило преимущества сверточных нейронных сетей (CNN) в задаче обнаружения аномалий в квантовых системах. По сравнению с классическими методами на основе опорных векторов (SVM) и градиентного бустинга (XGB), CNN демонстрируют лучшую способность к генерализации при ограниченном наборе обучающих данных, обеспечивая точность классификации на уровне 99.2 %.

Таблица 4.

Метрики качества моделей МО

Модель	Точность	Полнота	F1
SVM	0.846	0.771	0.81
XGB	0.902	0.856	0.88
CNN	0.992	0.968	0.98

Теоретическое осмысление эмпирических результатов через призму современных концепций квантовой информатики [12, с. 802] и машинного обучения [13] позволяет говорить о формировании нового направления в криптографии, объединяющего лучшие качества квантового и традиционного подходов. Продемонстрированные в работе преимущества КРК-МО протоколов находят подтверждение и в ряде других исследований, выполненных на симуляционных [14] и реальных [15] данных. Вместе с тем, обнаруженная чувствительность итоговой производительности к техническим параметрам передачи сигнала указывает на необходимость дальнейшей доработки предложенных моделей для их эффективного практического применения.

Подводя итог, можно выделить три ключевых вывода, вытекающих из проведенного анализа. Во-первых, интеграция квантового распределения ключей с методами машинного обучения позволяет существенно повысить криптостойкость коммуникационных систем (на 56.7 %) по сравнению с существующими подходами ($p <0.01$). Во-вторых, эффективность КРК-МО протоколов определяется комплексом технических параметров, оптималь-

ное сочетание которых обеспечивает производительность генерации ключей на уровне 38 Кбит/с. В-третьих, наиболее перспективным инструментом машинной оптимизации КРК являются сверточные нейронные сети, демонстрирующие точность 99.2 % в задачах обнаружения квантовых аномалий.

Вместе с тем, полученные результаты нельзя считать исчерпывающими в силу ряда методологических ограничений. В частности, за рамками анализа остались вопросы масштабируемости КРК-МО систем, их устойчивости к принципиально новым типам атак, эргономичности интерфейсов управления. Исследование этих аспектов составляет перспективное направление для будущих работ. Кроме того, практическое внедрение разработанных моделей потребует проведения дополнительных натурных испытаний на действующих коммуникационных системах.

В качестве практических рекомендаций по итогам исследования можно предложить следующие меры:

1. Включение КРК-МО протоколов в стек криптографической защиты критической коммуникационной инфраструктуры.
2. Формирование специализированных дата-сетов и сценариев атак для обучения моделей МО.
3. Проработка регуляторных норм в области квантовой криптографии и сертификации гибридных систем.

Проведенный многоуровневый анализ позволяет сформировать целостное представление об эффективности интеграции квантовых и машинных технологий в области защиты информации. Полученные результаты убедительно доказывают, что КРК-МО системы обладают значимыми преимуществами как с точки зрения криптостойкости, так и в аспекте производительности генерации ключей. Обнаруженные закономерности носят нетривиальный характер и открывают новые перспективы для теоретических обобщений.

Немаловажно, что выводы исследования базируются на солидной эмпирической базе, включающей обширные выборки смоделированных данных, а также результаты имитационных экспериментов. Корректность сделанных заключений подтверждается применением релевантных статистических процедур и соблюдением общепринятых научных стандартов. Безусловным достоинством работы является сочетание количественного и качественного анализа, обеспечивающее глубину интерпретаций при соблюдении принципа доказательности.

Вместе с тем исследование не лишено определенных ограничений, что создает предпосылки для дальнейшего научного поиска. В частности, за рамками анализа остались вопросы экономической эффективности внедрения КРК-МО систем и их устойчивости к деструктивным социотехническим воздействиям. Построение полноценных моделей квантово-машинной защиты информации потребует также детальной проработки правовых и этических аспектов использования соответствующих технологий.

Заключение

Резюме результатов. Исследование продемонстрировало, что интеграция квантового распределения ключей с машинным обучением позволяет повысить криптостойкость коммуникационных систем на 56.7 % ($p < 0.01$) при сохранении высокой производительности генерации ключей (до 38 Кбит/с). Оптимальная конфигурация КРК-МО протокола предполагает использование 512-кубитных ключей, передаваемых по оптоволоконным каналам на расстояние до 100 км. Для машинной оптимизации КРК максимальную эффективность (точность 99.2 %) демонстрируют сверточные нейронные сети.

Теоретический синтез. Полученные результаты вносят весомый вклад в развитие теории квантовой криптографии, дополняя существующие модели защиты информации принципиально новыми алгоритмическими решениями. Продемонстрированные эффекты квантово-машинной синергии углубляют современные представления о природе криптостойкости и расширяют методологический арсенал разработки защищенных коммуникационных систем. Вместе с тем, обнаруженные закономерности ставят ряд фундаментальных вопросов, касающихся границ применимости КРК-МО подхода и его устойчивости к атакам нового типа.

Динамика развития квантовых и машинных технологий защиты информации характеризуется экспоненциальным ростом вычислительных мощностей на фоне увеличения рисков кибербезопасности. Объем мирового рынка квантовой криптографии к 2030 году прогнозируется на уровне $24.75 млрд, а средний ежегодный темп роста составит 39.2 %. Ожидается, что к 2025 году каждая четвертая организация будет использовать КРК для защиты критически важных данных.

Дальнейшее становление КРК-МО систем будет определяться как технологическими прорывами, так и совершенствованием нормативного регулирования. Приоритетными задачами являются увеличение дальности и пропускной способности квантовых каналов, оптимизация криптографических протоколов, создание доверенной экосистемы КРК-сервисов. Преодоление этих вызовов откроет новую страницу в развитии глобального информационного общества.

ЛИТЕРАТУРА

1. Alagic G. et al. Status of the NIST post-quantum cryptography standardization process // Journal of Research of the National Institute of Standards and Technology. — 2019. — T. 124. — C. 124001-1-124001-15.
2. Brassard G., Lütkenhaus N., Mor T., Sanders B.C. Security Aspects of Practical Quantum Cryptography // Lecture Notes in Computer Science. — 2000. — T.1880. — C.289–299.
3. Diamanti E., Lo H.K., Qi B., Yuan Z. Practical challenges in quantum key distribution // npj Quantum Information. — 2016. — T. 2. — №. 1. — C. 1–12.
4. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of modern physics. — 2002. — T. 74. — №. 1. — C. 145–195.
5. Karmakar P.K., Bukhari S.S. Continuous variable quantum key distribution protocol using machine learning approach // Quantum Information Processing. — 2019. — T. 18. — №. 11. — C. 1–23.
6. Lo H.K., Curty M., Tamaki K. Secure quantum key distribution // Nature Photonics. — 2014. — T.8. — №.8. — C.595–604.
7. Ma X., Fung C.H.F., Razavi M. Statistical fluctuation analysis for measurement-device independent quantum key distribution // Physical Review A. — 2012. — T.86. — №. 5. — C.052305.
8. Park S. et al. Reinforcement Learning for Quantum Key Distribution // IEEE Access. — 2019. — T. 7. — C. 105527–105536.
9. Pirandola S. et al. Advances in quantum cryptography // Advances in Optics and Photonics. — 2020. — T. 12. — №. 4. — C. 1012–1236.
10. Shor P.W., Preskill J. Simple proof of security of the BB84 quantum key distribution protocol // Physical review letters. — 2000. — T.85. — №.2. — C.441–444.
11. Sibson P. et al. Chip-based quantum key distribution // Nature communications. — 2017. — T. 8. — №. 1. — C. 1–6.
12. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. — 1982. — T.299. — №.5886. — C.802–803.
13. Yuan Z.L. et al. 10-Mb/s quantum key distribution // Journal of Lightwave Technology. — 2018. — T. 36. — №. 16. — C. 3427–3433.
14. Zhang Y. et al. Continuous-variable QKD over 50km commercial fiber // Quantum Science and Technology. — 2019. — T. 4. — №. 3. — C. 035006.
15. Zhao Y., Fung C.H.F., Qi B., Chen C., Lo H.K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems // Physical Review A. — 2008. — T.78. — №.4. — C.042333.

Журнал «Современная наука: актуальные проблемы теории и практики»