ПРИМЕНЕНИЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЦИФРОВЫХ СИСТЕМАХ

М.М. Ходжамаммедов

Государственный энергетический институт Туркменистана, г. Мары, Туркменистан

Аннотация. В статье представлен комплексный научный анализ применения постквантовой криптографии как ключевого направления обеспечения информационной безопасности в условиях развития квантовых вычислений. Рассматриваются ограничения классических криптографических методов, обусловленные появлением квантовых алгоритмов, а также исследуются современные подходы к построению устойчивых криптосистем. Особое внимание уделено решеточным, кодовым и хэш-ориентированным алгоритмам, а также вопросам их практической интеграции в цифровые инфраструктуры. Обоснована необходимость перехода к криптографическим решениям нового поколения.

Ключевые слова: постквантовая криптография; квантовые вычисления; защита информации; криптографическая устойчивость; цифровая безопасность; алгоритмы; киберугрозы.

APPLICATION OF POST-QUANTUM CRYPTOGRAPHY FOR INFORMATION SECURITY IN DIGITAL SYSTEMS

M.M. Hojamammedow

State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. The paper presents a comprehensive scientific analysis of post-quantum cryptography as a key approach to ensuring information security in the context of quantum

computing development. The limitations of classical cryptographic methods caused by quantum algorithms are examined, and modern approaches to building quantum-resistant cryptosystems are analyzed. Particular attention is paid to lattice-based, code-based, and hash-based methods, as well as their practical integration into digital infrastructures. The necessity of transitioning to next-generation cryptographic solutions is substantiated.
Keywords: post-quantum cryptography; quantum computing; information security; cryptographic strength; digital security; algorithms; cyber threats.

Введение

Стремительное развитие цифровых технологий и переход к новым вычислительным парадигмам формируют качественно новые вызовы в области информационной безопасности. Одним из наиболее значимых факторов является развитие квантовых вычислений, способных радикально изменить существующие подходы к защите информации. В этих условиях традиционные криптографические алгоритмы постепенно утрачивают свою надежность, что обусловливает необходимость поиска альтернативных решений.

Появление квантовых алгоритмов, ориентированных на решение сложных математических задач, лежащих в основе современных криптосистем, создает предпосылки для их потенциальной компрометации. Это делает актуальным переход к новым криптографическим механизмам, способным обеспечить устойчивость к принципиально иным типам вычислительных атак.

Основная часть

Постквантовая криптография представляет собой перспективное направление, ориентированное на разработку алгоритмов, устойчивых к воздействию как классических, так и квантовых вычислительных средств. В отличие от традиционных методов, ее основой являются математические задачи, сохраняющие вычислительную сложность даже при использовании квантовых технологий.

Одним из наиболее активно развивающихся направлений является решеточная криптография. Данный подход базируется на сложных задачах многомерной геометрии, решение которых остается вычислительно трудоемким. Практическая значимость таких алгоритмов определяется их высокой производительностью и возможностью применения в различных криптографических протоколах.

Кодовые криптосистемы представляют собой еще одно важное направление. Их устойчивость основана на сложности декодирования случайных линейных кодов. Несмотря на значительные требования к объему ключевой информации, такие системы демонстрируют высокий уровень надежности и активно рассматриваются как кандидаты для стандартизации.

Хэш-ориентированные методы обеспечивают безопасность за счет использования криптографических хэш-функций. Они находят широкое применение в системах цифровой подписи и отличаются высокой степенью формальной обоснованности безопасности.

Современные исследования в области постквантовой криптографии направлены не только на разработку новых алгоритмов, но и на их адаптацию к существующим цифровым системам. Важным аспектом является обеспечение совместимости с действующими протоколами и инфраструктурой, что требует создания гибридных решений, сочетающих классические и постквантовые методы защиты.

Отдельного внимания заслуживает процесс международной стандартизации постквантовых алгоритмов. Ведущие научные организации активно проводят исследования и отбор наиболее перспективных решений, что подтверждает стратегическую значимость данного направления для глобальной информационной безопасности.

Заключение

Таким образом, постквантовая криптография является ключевым элементом формирования устойчивых систем защиты информации в условиях цифровой трансформации. Переход к новым криптографическим стандартам представляет собой необходимый этап эволюции информационной безопасности. Дальнейшее развитие данной области связано с совершенствованием алгоритмов, оптимизацией их реализации и интеграцией в современные цифровые инфраструктуры.

Список использованных источников

1. NIST. Post-Quantum Cryptography Standardization. 2023.
2. Bernstein D. Lattice-Based Cryptography. 2021.
3. Alagic G. Status Report on PQC. 2024.
4. Chen L. Post-Quantum Cryptography Report. 2022.

References

1. NIST. Post-Quantum Cryptography Standardization, 2023.
2. Bernstein D. Lattice-Based Cryptography, 2021.
3. Alagic G. PQC Status Report, 2024.
4. Chen L. Post-Quantum Cryptography Report, 2022.

Сведения об авторе

Ходжамаммедов М.М. – преподаватель кафедры информационных технологий, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com.

Information about the author

Hojamammedow M.M. – Lecturer of the Department of Information Technologies, State Energy Institute of Turkmenistan, Mary, Turkmenistan, mekanhoja2021@gmail.com.