

В настоящее время в технологически развитых странах мира, главным образом в США, Китае, России и странах Евросоюза, запланирован переход к постквантовой криптографии. Актуальность упомянутого перехода подтверждается требованиями национальной программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства Российской Федерации от 28 июня 2017 г. № 1632-р. В этой программе «обеспечение устойчивости и безопасности функционирования информационной инфраструктуры и сервисов передачи, обработки и хранения больших объемов данных», в том числе национальных блокчейн-экосистем и платформ, является одной из пяти ключевых целей Проекта «Информационная безопасность». При этом акцент делается именно на устойчивости к новым атакам злоумышленников с использованием так называемого релевантного или значимого квантового компьютера (*Cryptographically Relevant Quantum Computer, CRQC*).

В настоящем учебно-методическом пособии рассмотрено возможное решение задачи параметрического выбора постквантовых криптопримитивов на основе целочисленных решеток (*lattice-based cryptography*), кодов, исправляющих ошибки (*code-based cryptography*), многочленов от многих переменных (*multivariate cryptography*), криптографических хеш-функций (*hash-based cryptography*), изогений суперсингулярных эллиптических кривых (*supersingular isogeny-based cryptography*) и пр. Приведены соответствующие примеры и выработанный ряд полезных рекомендаций.

Пособие представляет определенный теоретический и практический интерес для специалистов в области информационных технологий и киберустойчивости Цифровой экономики Российской Федерации.

Введение

Глава 1. Модели и методы анализа квантовой устойчивости блокчейн-экосистем и платформ цифровой экономики Российской Федерации

- 1.1. Метод оценки квантовой устойчивости блокчейн-экосистем и платформ цифровой экономики Российской Федерации
 - 1.1.1. Вербальная и математическая задача исследования
 - 1.1.2. Предлагаемый метод оценки квантовой устойчивости блокчейна
 - 1.1.3. Разработка платформы «Квант-К»
- 1.2. Реализация квантового алгоритма Шора на квантовой схеме
 - 1.2.1. Квантовый алгоритм факторизации Шора
- 1.3. Реализация квантового алгоритма поиска Гровера на квантовой схеме
 - 1.3.1. Разработка алгоритма криптоанализа системы асимметричного шифрования
 - 1.3.2. Разработка квантового алгоритма криптоанализа системы Эль-Гамала
- 1.4. Выработка требований к инструментальным средствам квантового криптоанализа
 - 1.4.1. Математические пакеты Maple и Mathematica
 - 1.4.2. Эмуляторы квантовых вычислений
 - 1.4.3. Квантовые компьютеры
 - 1.4.4. Промежуточные итоги

Глава 2. Модели и методы синтеза квантово-устойчивых блокчейн-экосистем и платформ цифровой экономики Российской Федерации

- 2.1. Эталонная модель квантово-устойчивой блокчейн-экосистемы или платформы цифровой экономики Российской Федерации
 - 2.1.1. Международный технический комитет ИСО/ТК 307 (ISO/TC 307)
 - 2.1.2. Международный союз электросвязи (МСЭ-Т)
 - 2.1.3. Институт стандартов NIST США
 - 2.1.4. Европейское агентство ENISA
 - 2.1.5. Возможная модель квантово-устойчивой блокчейн-платформы
- 2.2. Постквантовые криптопримитивы для квантово-устойчивых блокчейн-экосистем и платформ
 - 2.2.1. Постквантовые криптопримитивы
- 2.3. Метод параметрического выбора постквантовых криптопримитивов
- 2.4. Примеры создания и пилотного внедрения квантово-устойчивых блокчейнов

Заключение

Литература

Сведения об авторе