

Оглавление

Введение	9
Глава 1. Постановка задачи на разработку постквантовых алгебраических алгоритмов ЭЦП с малыми размерами и высокой стойкостью	14
1.1. Оценка достаточности международных постквантовых алгоритмов ЭЦП	16
1.1.1. Постквантовый алгоритм CRYSTALS-Dilithium (FIPS 204 — ML-DSA)	16
1.1.2. Постквантовый алгоритм FALCON (FIPS 206 — FN-DSA) ..	16
1.1.3. Постквантовый алгоритм SPHINCS+ (FIPS 205 — SLH-DSA)	17
1.1.4. Постквантовые алгоритмы XMSS и LMS	18
1.1.5. Постквантовый алгоритм Rainbow.	20
1.2. Достоинства и недостатки известных международных алгоритмов постквантовой ЭЦП	20
1.3. Оценка достаточности отечественных постквантовых алгоритмов ЭЦП	22
1.3.1. Постквантовый алгоритм «Шиповник»	22
1.3.2. Постквантовый алгоритм «Крыжовник»	23
1.3.3. Другие постквантовые алгоритмы электронной подписи	23
1.4. Предпосылки создания нового метода построения постквантовых ЭЦП на основе КНАА с двумя скрытыми группами ...	24
1.5. Вербальная и математическая постановка задачи исследования ...	29
Выводы по главе 1	32
Глава 2. Метод построения постквантовых алгебраических алгоритмов ЭЦП с малыми размерами и высокой стойкостью	33
2.1. Выбор и обоснование базовой схемы построения постквантовых алгебраических алгоритмов ЭЦП на основе КНАА с двумя скрытыми группами	33

2.2. Определение основных математических свойств используемого алгебраического носителя для стойких постквантовых ЭЦП	37
2.3. Задание базовых алгоритмов генерации ключей, формирования и верификации подписи в постквантовых алгебраических алгоритмах ЭЦП с одним проверочным уравнением	41
2.3.1. Базовый алгоритм генерации ключей	41
2.3.2. Базовый алгоритм генерации постквантовой ЭЦП	42
2.3.3. Базовый алгоритм верификации постквантовой ЭЦП	44
2.3.4. Доказательство корректности схемы постквантовой ЭЦП ...	45
2.3.5. Способ оценивания стойкости алгебраических алгоритмов ЭЦП к атакам на основе известных подписей	46
2.3.6. Основные преимущества предлагаемого способа построения стойких постквантовых ЭЦП с малыми размерами подписи и открытого ключа.	48
2.4. Возможность использования матричной алгебры 3×3 для создания алгебраического алгоритма ЭЦП альтернативного типа ..	49
2.4.1. Базовый алгоритм альтернативного типа электронной подписи	52
2.4.2. Базовый альтернативный алгоритм генерации ЭЦП	54
2.4.3. Базовый альтернативный алгоритм верификации ЭЦП	55
2.4.4. Доказательство корректности алгоритма ЭЦП альтернативного типа	56
2.4.5. Особенности альтернативного базового алгебраического алгоритма ЭЦП	57
Выводы по главе 2	58

Глава 3. Постквантовые алгебраические алгоритмы ЭЦП на основе вычислительной трудности решения больших систем степенных уравнений

59

3.1. Варианты задания четырехмерных КНАА для построения постквантовых ЭЦП	59
3.2. Постквантовый алгебраический алгоритм ЭЦП первого типа	62
3.2.1. Алгоритм генерации ЭЦП первого типа	63
3.2.2. Алгоритм верификации ЭЦП первого типа	64
3.2.3. Доказательство корректности алгоритма ЭЦП первого типа	66

3.3. Постквантовый алгебраический алгоритм ЭЦП второго типа	66
3.3.1. Алгоритм генерации ЭЦП второго типа	67
3.3.2. Алгоритм верификации ЭЦП второго типа	69
3.3.3. Доказательство корректности алгоритма ЭЦП второго типа	70
3.4. Постквантовый алгебраический алгоритм ЭЦП третьего типа	70
3.4.1. Алгоритм генерации ЭЦП третьего типа	71
3.4.2. Алгоритм верификации ЭЦП третьего типа	73
3.4.3. Доказательство корректности алгоритма ЭЦП третьего типа	74
3.5. Характеристики стойкости постквантовых алгебраических алгоритмов ЭЦП	74
3.6. Использование хаотических отображений для усиленной рандомизации ЭЦП	78
3.7. Оценка стойкости постквантовых алгебраических алгоритмов ЭЦП к компьютерным атакам с применением квантового компьютера и суперЭВМ фон Неймана сверхвысокой производительности	81
3.7.1. Прямая атака на секретные параметры алгоритмов	81
3.7.2. Атака на основе множества известных подписей	82
3.7.3. Квантовые атаки Гровера и Шора	82
3.7.4. Сочетанные и разнородные массовые атаки	83
3.7.5. Способ оценивания стойкости постквантовой ЭЦП на основе КНАА с двумя скрытыми группами к атакам на базе известных подписей	84
Выводы по главе 3	86

Глава 4. Методика построения стойких постквантовых ЭЦП на базе КНАА с двумя скрытыми группами (КНАА-2-ЭЦП) 88

4.1. Основные цели и задачи предлагаемой методики построения КНАА-2-ЭЦП	88
4.1.1. Назначение методики построения КНАА-2-ЭЦП	88
4.1.2. Рекомендации лучшей практики построения постквантовых ЭЦП	89
4.1.3. Используемые в методике построения КНАА-2-ЭЦП сокращения и обозначения	90

4.2. Выбор и обоснование наборов параметров и целевых показателей КНАА-2-ЭЦП.....	91
4.2.1. Категории криптографической стойкости КНАА-2-ЭЦП....	91
4.2.2. Наборы параметров и основные числовые показатели КНАА-2-ЭЦП	92
4.2.3. Роль и значение длины подписи в методике КНАА-2-ЭЦП..	93
4.2.4. Обоснование выбора параметров КНАА-2-ЭЦП	94
4.3. Требования к инженерной реализации КНАА-2-ЭЦП	95
4.3.1. Постоянное время выполнения.....	95
4.3.2. Формирование исходной случайности на основе хаотического отображения.....	96
4.3.3. Идентификация объектов и формальный синтаксис.....	97
4.3.4. Профили применения алгоритма КНАА-2-ЭЦП	98
4.3.5. Основные требования безопасности	99
4.4. Программа тематических исследований и испытаний КНАА-2-ЭЦП.....	101
4.4.1. Положительный контрольный пример.....	101
4.4.2. Отрицательный контрольный пример и тест согласованности ключей	101
4.4.3. Сокращенный многоцикловый тест.....	102
4.4.4. Контрольный тест производительности «1000 Verify».....	103
4.4.5. Тест рандомизации для КНАА-2-ЭЦП.....	104
4.4.6. Критерии успешного прохождения испытаний КНАА-2-ЭЦП	104
4.5. Возможные направления развития КНАА-2-ЭЦП	106
4.5.1. Рекомендации стандартов постквантовых алгоритмов ЭЦП	106
4.5.2. Оценки производительности при реализации КНАА-2-ЭЦП на известных аппаратных платформах.....	107
4.5.3. Возможные сценарии интеграции КНАА-2-ЭЦП в прикладные системы.....	108
4.5.4. Рекомендации по регистрации версий КНАА-2-ЭЦП и прохождению протокола автоматического тестирования криптографических модулей в программном и аппаратном обеспечении.....	111

4.5.5. Возможные рекомендации по внедрению КНАА-2-ЭЦП в национальные блокчейн-экосистемы и платформы	112
Выводы по главе 4	114

Глава 5. Программная архитектура программного комплекса для встраивания КНАА-2-ЭЦП для обеспечения квантовой устойчивости цифровых платформ экономики данных РФ на примере национальных блокчейн-систем	115
5.1. Концептуальная модель типовой блокчейн-экосистемы в условиях компьютерных атак с применением квантового компьютера и суперЭВМ фон Неймана высокой и сверхвысокой производительности.	116
5.2. Роль и место постквантовых криптопримитивов в обеспечении безопасности и киберустойчивости национальных блокчейн-экосистем и платформ	120
5.3. Модель угроз безопасности информации в национальных блокчейн-экосистемах и платформах.	123
5.4. Математическая модель деградации устойчивости блокчейн-систем в условиях компьютерных атак с применением квантового компьютера.	127
5.4.1. Постановка задачи и исходные допущения.	127
5.4.2. Утверждения и вспомогательные леммы.	128
5.4.3. Градуировка устойчивости и рекомендации по защите	136
5.5. Методы мониторинга деградации на основе фильтра Калмана.	138
5.5.1. Модель мониторинга и оценивания скрытого состояния сети	138
5.5.2. Применение модели в операционном мониторинге.	141
5.6. Решение оптимизационных задач обеспечения устойчивости функционирования блокчейн-систем на основе машины Изинга или решателя задач бинарной оптимизации	146
5.6.1. Постановка задачи квадратической бинарной оптимизации	147
5.6.2. Гамильтониан и влияние атак	148
5.6.3. Коррекция квантового отжига и штрафные функции	149
5.6.4. Аппаратная симуляция квантового отжига.	151

5.7. Структурно-функциональная схема программного комплекса для обеспечения квантовой устойчивости национальных блокчейн-экосистем и платформ на основе разработанного метода построения постквантового алгебраического алгоритма ЭЦП	153
5.8. Рекомендации по дальнейшему развитию программной архитектуры программного комплекса для обеспечения квантовой устойчивости национальных блокчейн-экосистем и платформ на основе разработанного метода построения постквантового алгебраического алгоритма ЭЦП	157
Выводы по главе 5	161
Заключение	162
Список используемых терминов	164
Список используемых сокращений	166
Список литературы	168
Дополнительная литература	187
Публикации в изданиях, проиндексированных в Web of Science/SCOPUS	189
Монографии	190
Свидетельства о регистрации программы для ЭВМ	191
Приложение А	193
Приложение Б	241
Приложение В	244
Об авторе	251