Комплекс методик совершенствования алгоритмов постквантового шифрования основанных на математической теории решеток

Н.А. Клейменов, К.З. Билятдинов

***Аннотация* — представлены методологические решения по совершенствование процесса анализа и параметрического выбора постквантового шифрования на основе математических решеток. Предлагается комплекс взаимосвязанных методик оптимизации, направленный на повышение производительности и криптографической стойкости криптографических примитивов.**

Комплекс методик формализует процесс совершенствования алгебраической структуры, лежащей в основе современных стандартов, таких как CRYSTALS-Kyber. В рамках комплекса разработаны три целевые методики: модификация алгебраического идеала для ускорения вычислений, управление размерностью матриц для усиления стойкости и введение нелинейных искажений для противодействия специализированным атакам. Каждая методика содержит формализованную последовательность действий, систему верифицируемых показателей эффективности и четкие критерии оценки результатов оптимизации.

***Ключевые слова* — криптография, постквантовая криптография, математические решетки, ключи, шифрование.**

I. Введение

В современной криптографии все больше прослеживается тенденция поиска новых решений, которые обеспечивают безопасность как к классическим, так и к квантовым атакам [1]. Наиболее перспективным считается постквантовое шифрование, основанное на математической теории решеток, что подтверждено их стандартизацией NIST [2].

Основу этих методов составляют структурированные решетки, порождаемые кольцами многочленов, где эффективность и безопасность напрямую определяются свойствами алгебраического кольца (подробное описание алгебраической структуры представлено в разделе III).

Актуальность работы обусловлена необходимостью оптимизации и анализа параметров криптографических схем для достижения оптимального баланса между безопасностью и скоростью.

В данной работе предлагается комплекс методик по совершенствованию алгоритмов постквантового шифрования основанных на математической теории решеток через целенаправленную модификацию структуры алгебраического кольца. Основное внимание уделяется разработке системы объективных метрик, позволяющих количественно оценивать влияние любых изменений в структуре кольца на криптографические свойства схемы. Такой подход обеспечивает комплексный подход к оптимизациям и улучшению постквантового шифрования.

Практическая значимость работы заключается в возможности применения разработанных методик для оптимизации параметров стандартизированных алгоритмов Kyber и Dilithium [3,4], а также для ускорения разработки новых криптографических решений. Предлагаемый системный подход позволяет сократить время на поиск оптимальных параметров алгебраического кольца и обеспечивает набор готовых решений по поиску оптимальных параметров для модификации криптографических схем постквантового шифрования.

II. Основы исследования и постановка задачи

Актуальность совершенствования алгоритмов постквантового шифрования предопределяют необходимость применения системного подхода к анализу результатов научных исследований [5, 6, 7], которые потенциально могут быть полезны для модернизации исследуемых Алгоритмов.

Важно выявить и определить основные параметры алгебраического кольца, в котором происходят вычисления в рамках постквантового шифрования. Особое внимание уделить безопасности, эффективности и сложности.

Вышеизложенное подтверждает потенциальные возможности эффективного использования современных научных достижений при совершенствовании процесса анализа и параметрического выбора постквантового шифрования основанных на математической теории решеток.

Отсюда целесообразно сформулировать три взаимосвязанные задачи исследования:

1. Определить и систематизировать математические основы и принципы модификации алгебраического кольца для совершенствования алгоритмов постквантового шифрования на основе решеток.

2. Разработать комплекс методик совершенствования алгоритмов постквантового шифрования, включающий три взаимосвязанные методики оптимизации:

модификацию алгебраического идеала, управление размерностью матриц и введение нелинейных искажений. Применение комплекса методик должно быть направлено на решение задачи повышения производительности шифров при сохранении или усилении их криптографической стойкости.

3. Состав и содержание методик должны обеспечивать их практическую применимость для разработчиков криптографических решений, что включает формализацию последовательности действий, разработку верифицируемых показателей эффективности и критериев оценки результатов оптимизации.

III. Алгебраическое кольцо и задача обучения с ошибками

Для исследования было взято алгебраическое кольцо, которое используется в протоколе CRYSTALS-Kyber. Это решение постквантового шифрования, которое построено на модульной задаче обучения с ошибкой. Данный протокол является финалистом NIST и стандартом постквантового шифрования.

Задача обучения с ошибкой в модулях (Module-LWE) [8] является математической проблемой в рамках теории решеток. Она заключается в нахождении секретного вектора многочленов с малыми коэффициентами на основе системы линейных уравнений над кольцом многочленов, в которые добавлены случайные ошибки. В протоколе CRYSTALS-Kyber данная задача выражается соотношением:

$$t = A * s + e$$

где A – случайная матрица размерности $k \times k$, где каждый элемент — многочлен в кольце;

s – вектор, который является секретным ключом;

e - вектор который является динамическом шумом который используется для каждой криптографической операции с целью увеличения безопасности;

В протоколе CRYSTALS-Kyber используется кольцо:

$$R_q = Z_q[X]/(x^n + 1)$$

где Z_q – это конечное кольцо по модулю q. Все коэффициенты в многочленах — это целые числа от 0 до q-1;

q - это большой модуль, часто простое число (в Kyber 3329) так же могут использоваться степень двойки;

$Z_q[X]$ — это множество всех многочленов с коэффициентами из Z_q;

$(x^n + 1)$ – это идеал, порожденный многочленом. На практике это означает, что мы работаем с многочленами по модулю $(x^n + 1)$;

Для составления методик мы будем использовать основные параметра данного алгебраического кольца.

IV. Методика оптимизации через модификацию идеала. Сведение к кольцу с альтернативным идеал

Назначение Методики: повышение эффективности выполнения криптографических операций (шифрование, дешифрование) посредством замены алгебраического идеала, порождающего кольцо, на идеал, допускающий применение более быстрых алгоритмов.

Элементом криптосистемы выступает алгебраическая структура — кольцо многочленов [9] R_q (определение и свойства кольца приведены в разделе III), в котором выполняются все базовые операции..

Принятое ограничение: Исходный идеал $(x^n + 1)$ [10] может не являться оптимальным для эффективной реализации арифметики на всех типах вычислительных архитектур.

Допущение: существуют альтернативные идеалы, которые при сохранении требуемого уровня криптографической стойкости позволяют повысить эффективность вычислений за счет более простой структуры.

В Методике установлены следующие обозначения:

$R_q = Z_q[X]/(x^n + 1)$ – исходное алгебраическое кольцо, используемое в криптосистеме Kyber;

$I = (x^n + 1)$ - исходный идеал, определяющий структуру кольца;

$I` = (x^m - a)$ - новый идеал, предлагаемый для замены;

$Perf(R_q)$ – показатель производительности (оп/с) операций в исходном кольце;

$Perf(R_q`)$ – показатель производительности операций в новом кольце;

$Sec(R_q)$ – уровень стойкости (бит) исходной схемы;

$Sec(R_q`)$ - уровень стойкости модифицированной; схемы.

$Memory(R_q)$ – объем памяти (байт), используемый для представления элементов исходного кольца;

$Memory(R_q`)$ – объем памяти, используемый для представления элементов нового кольца;

$CompatibleOperation$ - количество криптографических операций, оставшихся корректными после модификации;

$TotalOperation$ – общее количество криптографических операций в схеме;

K_{mul} - коэффициент эффективности умножения;

K_{mem} - коэффициент эффективности памяти;

K_{sec} - коэффициент сохранения стойкости;

K_{comp} - коэффициент совместимости.

Краткая последовательность действий и расчетов при выполнении Методики:

1. Определение целевого компонента. Выявление в схеме алгебраического кольца R_q, используемого для полиномиальных операций.

2. Выбор альтернативного идеала. Анализ и выбор нового идеала $I`$, который допускает применение более быстрых алгоритмов (например, на основе, быстрого преобразование Фурье [11]).

3. Построение модифицированного кольца. Конструирование нового кольца $R_q` = Z_q[X]/I`$.

4. Адаптация криптографических операций. Пересчет всех операций исходной схемы (генерация ключей, шифрование, дешифрование) для работы в $R_q`$.

5. Верификация и расчет показателей (формулы 1-4).

5.1 Коэффициент эффективности умножения K_{mul}:

$$K_{mul} = Perf(R_q`)/Perf(R_q)$$

(1)

5.2. Коэффициент эффективности памяти K_{mem}:

$$K_{mem} = Memory(R_q`)/Memory(R_q)$$

(2)

5.3. Коэффициент сохранения стойкости (K_{sec}):

$$K_{sec} = Sec(R_q`)/Sec(R_q)$$

(3)

5.4. Коэффициент совместимости (K_{comp}):

$$K_{comp} = CompatibleOperation/TotalOperation)$$

(4)

6.. Вывод по результатам оценки эффективности модификации производится на основании следующих эвристических критериев. Предлагаемые пороговые значения не являются строго доказанными, а сформулированы на основе общепринятых в области постквантовой криптографии инженерных допущений:

6.1. Если $K_{mul} > 1, K_{mem} \leq 1, K_{sec} \approx 1$ и $K_{comp} \approx 1$ – то модификация признается успешной и целесообразной. Производительность системы повысилась при сохранении требуемого уровня стойкости и корректности.

6.2. Если $K_{mul} > 1$, но $K_{sec} < 1, K_{comp} < 1$ – то система находится в зоне риска. Производительность достигнута за счет снижения стойкости или корректности, требуется пересмотр параметров.

6.3. Если $K_{mul} \leq 1$ – то модификация неудачна. Внесенные изменения не улучшили или ухудшили производительность системы, их применение нецелесообразно.

7. При необходимости выполнить сравнение с базовыми требованиями по производительности и стойкости. Составить рейтинг эффективности различных идеалов и представить результаты оценки для выбора оптимальной конфигурации.

Для получения численных значений коэффициентов $K_{mul}, K_{mem}, K_{sec}, K_{comp}$ необходимо выполнить экспериментальную реализацию выбранного альтернативного идеала на целевой вычислительной архитектуре с последующим профилированием производительности и оценкой стойкости. В рамках настоящей работы предлагаемый подход ограничивается формализацией методики, оставляя ее экспериментальную валидацию для последующих исследований.

Методика отражена на (Рис. 1).

V. Методика оптимизация через управление размерностью матриц

Назначение повышение криптографической стойкости системы посредством вложения исходного алгебраического кольца в кольцо большей размерности, что увеличивает сложность решеточных атак.

Элементом криптосистемы выступает размерность n кольца R_q (описание кольца см. в разделе III), которая определяет размерность матриц и решето к в схемах на основе LWE/RLWE..

Принятое ограничение: Атаки на основе редукции решеток (например, BKZ) являются наиболее практичными для схем на решетках, и их сложность напрямую зависит от размерности.

Допущение: Увеличение размерности алгебраической структуры напрямую повышает сложность решения соответствующей задачи обучения с ошибками (LWE) для криптоаналитика.

В Методике установлены следующие обозначения:

n – исходная размерность кольца R_q;

m – новая, увеличенная размерность целевого кольца($m > n$);

q - исходный модуль;

Q – новый модуль, возможно, отличный от q;

$Sec(n)$ - уровень стойкости (бит) исходной схемы с размерностью n.

$Sec(m)$ - уровень стойкости модифицированной схемы с размерностью m .

$Cycles(n)$ – количество вычислительных циклов для операций в исходной схеме;

$Cycles(m)$ – количество вычислительных циклов для операций в модифицированной схеме;

$Memory(n)$ – объем памяти (байт), используемый исходной схемой;

$Memory(m)$ - объем памяти, используемый модифицированной схемой;

$SuccessfulEmbeddings$ – количество успешных применений отображения вложения;

$TotalOperations$ – общее количество операций, требующих вложения;

K_{stiff} - коэффициент прироста стойкости;

K_{cpu} - коэффициент роста вычислительной нагрузки;

K_{ram} - коэффициент роста памяти;

K_{embed} - коэффициент эффективности вложения.

Краткая последовательность действий и расчетов при выполнении Методики:

1. Определение базовых параметров. Фиксация исходной размерности n и модуля q анализируемой схемы.

2. Выбор новой размерности и модуля. Обоснованный выбор новых параметров m и Q для увеличения сложности атак.

3. Построение вложения. Создание инъективного отображения [12] $\phi : R_q \to R_{Q`}$, позволяющего работать с исходными данными в пространстве большей размерности.

4. Адаптация схемы. Перенос всех вычислений в кольцо большей размерности $R_Q = Z_Q[Y]/(Y^m + 1)$

5. Верификация и расчет показателей (формулы 1-4).

5.1. Коэффициент эффективности умножения K_{mul}:

$$K_{stiff} = Sec(m) - Sec(n)$$

(1)

5.2. Коэффициент эффективности памяти K_{mem}:

$$K_{cpu} = Cycles(m)/\ Cycles(n)$$

(2)

5.3. Коэффициент сохранения стойкости K_{sec}:

$$K_{ram} = Memory(m) - Memory(n)$$

(3)

5.4. Коэффициент совместимости K_{comp}:

$$K_{embed} = SuccessfulEmbeddings/TotalOperation$$

(4)

6. Вывод по результатам оценки целесообразности увеличения размерности производится на основании следующих эвристических критериев. Указанные пороговые значения представляют собой ориентировочные границы, выработанные на основе экспертной оценки и требующие уточнения применительно к конкретной схеме и условиям эксплуатации:

6.1. Если $K_{stiff} > 0, K_{cpu}$ и K_{ram} находятся в пределах допустимого порога, а $K_{embed} \approx 1$ – то модификация признается успешной и целесообразной. Стойкость системы повышена при приемлемых затратах и сохранении корректности.

6.2. Если $K_{stiff} > 0, K_{cpu}$ и K_{ram} превышают допустимый порог – то система требует оптимизации. Рост стойкости нивелируется чрезмерным падением производительности, необходим поиск компромиссных параметров (m, Q).

6.3. Если $K_{stiff} \leq 0$ или $K_{embed} < 1$ – то модификация неудачна. Увеличение размерности не привело к повышению стойкости или нарушило корректность работы схемы.

7. При необходимости выполнить сравнение с базовыми требованиями по стойкости и производительности.

Приведенные коэффициенты $K_{stiff}, K_{cpu}, K_{ram}, K_{embed}$ требуют численной конкретизации через экспериментальное моделирование работы модифицированной схемы. Поскольку выбор новых параметров m и Q напрямую влияет на производительность и стойкость, практическое применение методики предполагает проведение вычислительных экспериментов, не входящих в объем настоящей работы.

Методика отражена на (Рис. 2).

VI. Методика введение нелинейных искажений.

Назначение методики: усиление стойкости системы к алгебраическим и статистическим атакам посредством введения нелинейного преобразования в структуру данных, нарушающего её линейный характер.

Элементом криптосистемы выступает линейная операция в кольце R_q (описание алгебраической структуры дано в разделе III), которая лежит в основе доказуемой безопасности LWE/RLWE.

Принятое ограничение: Линейность операций является уязвимостью, которая может эксплуатироваться специализированными криптоаналитическими методами.

Допущение: Введение контролируемой нелинейности в вычисления не нарушает корректность работы криптографического протокола, но существенно усложняет применение к нему стандартных методов криптоанализа.

Введение нелинейных биективных функций изменяет алгебраическую структуру схемы, применение нелинейного преобразования выводит модифицированную схему за рамки стандартных моделей доказуемой безопасности. В настоящей работе модификация рассматривается как эвристическое усиление, направленное против конкретных алгебраических и статистических атак, эксплуатирующих линейность исходной конструкции. Предлагаемая методика не претендует на сохранение редукции к LWE/RLWE в общем случае, однако позволяет оценить достигнутый уровень нелинейности, корректность и вычислительные затраты. Для сценариев, где сохранение доказуемой безопасности является критическим, методика предусматривает возможность выбора нелинейной функции, являющейся автоморфизмом кольца, что позволяет сохранить совместимость с моделью LWE/RLWE. Во всех остальных случаях безопасность модифицированной схемы требует отдельного анализа, не входящего в рамки настоящего исследования.

В Методике установлены следующие обозначения:

a - многочлен в кольце R_q;

F - нелинейная биективная функция, применяемая к коэффициентам многочлена;

F^{-1} обратная функция к F;

$LinComplexity$ – оценка линейной сложности (условные единицы) исходной схемы;

$LinComplexity_F$ – оценка линейной сложности модифицированной схемы после применения нелинейного преобразования;

$CorrectOperations$ – количество корректно выполненных операций в модифицированной схеме;

$TotalOperations$ – общее количество операций в схеме;

$T(F)$ – время выполнения операций с применением функции F;

$T(base)$ – время выполнения базовых операций;

$BijectivePoints$ – количество точек в $\mathbb{Z}_q$, где функция F является биекцией;

$TotalPoints$– общее количество точек в $\mathbb{Z}_q$;

K_{nonlin} - коэффициент нелинейности;

K_{corr} - коэффициент корректности;

$K_{overhead}$ – коэффициент вычислительных затрат;

K_{biject}– коэффициент биективности.

Краткая последовательность действий и расчетов при выполнении Методики:

1. Определение точки приложения. Выбор этапа криптографического протокола (генерация секретного ключа), куда будет встроена нелинейность.

2. Выбор нелинейной функции. Выбор биективной функции [11] $F: \mathbb{Z}_q \to \mathbb{Z}_q$ (например, $f(x) = x^3 \bmod q$), которая является нелинейной и вычислительно эффективной.

3. Интеграция в схему. Модификация протокола: применение F к целевым данным (например, $S_{new} = F(s)$) на этапе шифрования/генерации ключа и F^{-1} – на

этапе дешифрования.

4. Проверка корректности. Тестирование модифицированной схемы на корректность работы: для любого сообщения $Decrypt(Enctypt(message)) = message$.

5. Верификация и расчет показателей (формулы 1-4).

5.1. Коэффициент нелинейности K_{nonlin}

$$K_{nonlin} = LinComplexity_{F}/LinComplexity \quad (1)$$

5.2. Коэффициент эффективности памяти K_{corr}:

$$K_{corr} = CorrectOperations/TotalOperations \quad (2)$$

5.3. Коэффициент сохранения стойкости $K_{overhead}$:

$$K_{overhead} = T(F)/T(base) \quad (3)$$

5.4. Коэффициент совместимости K_{biject}:

$$K_{biject} = BijectivePoints/TotalOperation \quad (4)$$

6. Вывод по результатам оценки целесообразности увеличения размерности на основании следующих критериев, носящих эвристический характер:

6.1. Если $K_{corr} \approx 1, K_{nonlin} > 1, K_{biject} \approx 1$ и $K_{overhead} \approx 1$ – то модификация признается успешной и перспективной. Стойкость системы к линейному криптоанализу повышена при сохранении корректности и биективности.

6.2. Если $K_{corr} \approx 1,$ но $K_{nonlim} \approx 1$ – то система не получила значимых улучшений. Внесенная нелинейность не усложнила задачу криптоаналитику, требуется выбор более эффективной функции

6.3. Если $K_{corr} < 1$ или $K_{biject} < 1$ – то модификация неудачна и неприменима. Нарушена корректность работы криптографического протокола или функция не является биективной, что делает систему неработоспособной.

7. При необходимости выполнить сравнение с альтернативными нелинейными функциями по критериям "Сложность-Биективность-Быстродействие". Составить рейтинг функций F и представить результаты оценки для дальнейшего углубленного исследования.

В настоящей работе методика представлена на уровне формального описания последовательности действий и системы оценочных коэффициентов. Применение методики к конкретной криптографической схеме (например, CRYSTALS-Kyber) требует выбора конкретной нелинейной функции F,реализации модифицированного протокола и выполнения натурных или имитационных экспериментов для получения численных значений коэффициентов $K_{corr}, K_{nonlin}, K_{overhead}, K_{biject}$. Такая реализация представляет собой отдельную исследовательскую задачу, выходящую за рамки настоящей работы, целью которой является разработка универсального инструментария оценки, а не демонстрация его применения на конкретном примере.

Методика отражена на (Рис. 3).

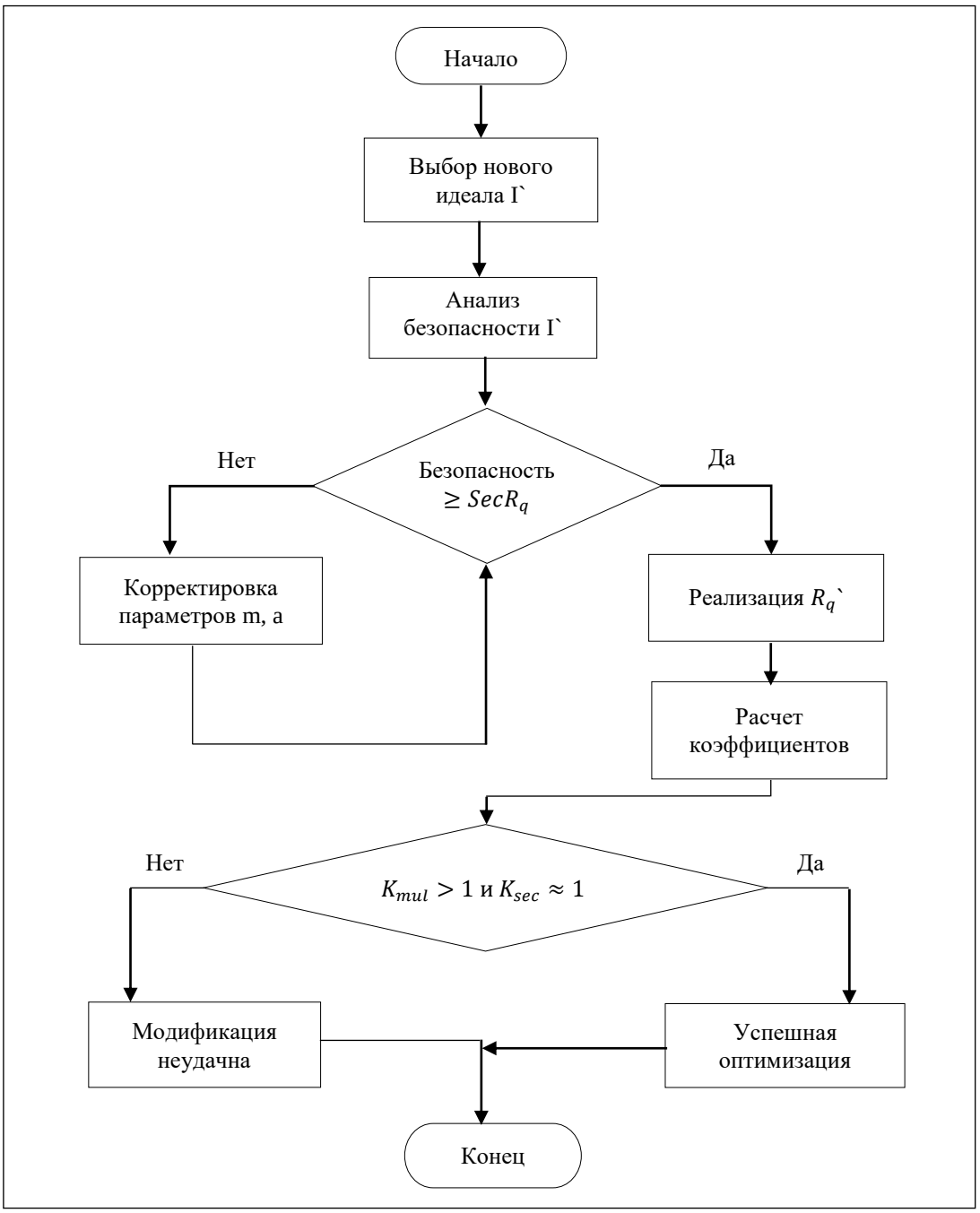

Рис. 1 – Схема методики оптимизации через модификацию идеала.
Сведение к полю меньшей размерности

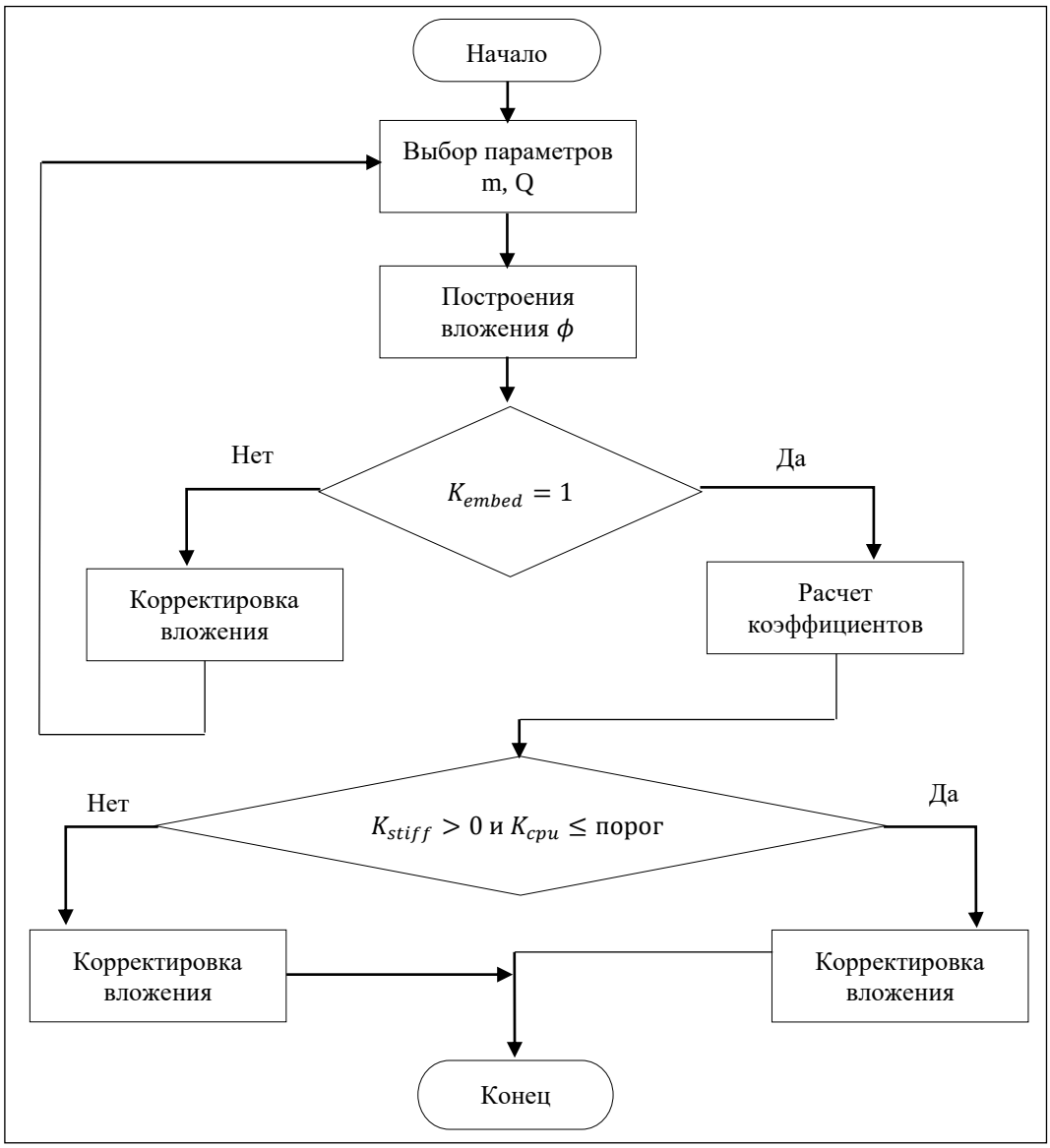

Рис. 2 – Схема методики оптимизации через управление размерностью матриц

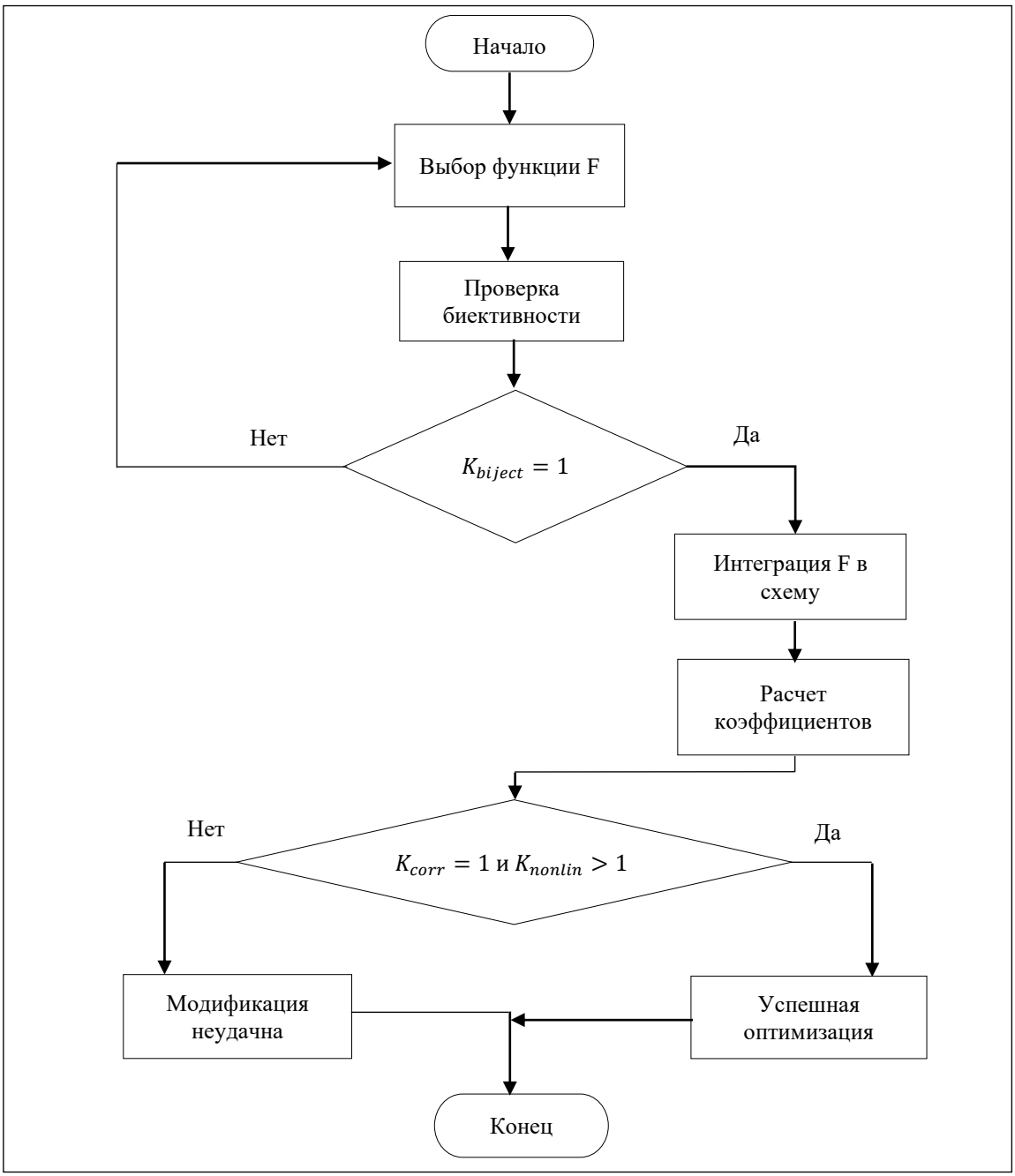

Рис. 3 – Схема методики введения нелинейных искажений

Таблица 1

Критерии успешности для всех методик

Параметр	Модификация идеала	Управление размерностью	Нелинейные искажения
Назначение	Повышение эффективности вычислений	Увеличение криптографической стойкости	Усложнение линейного криптоанализа
Основные параметры	Идеал $(x^n + 1)$	Размерность кольца n	Линейная структура операций в R_q
Ключевые операции	Замена идеала, адаптация арифметики	Вложение $\phi : R_q \to R_Q$, перенос вычислений	Применение F к коэффициентам, интеграция в протокол
Контрольные точки	$K_{sec} \approx 1$, $K_{mul} > 1$	$K_{embed} = 1$, $K_{stiff} > 0$	$K_{biject} = 1$, $K_{corr} = 1$
Критерии успеха	Рост производительности при сохранении стойкости	Рост стойкости при приемлемых затратах	Увеличение нелинейности при сохранении корректности
Выходные коэффициенты	$K_{mul}, K_{mem}, K_{sec}, K_{comp}$	$K_{stiff}, K_{cpu}, K_{ram}, K_{embed}$	$K_{nolin}, K_{corr}, K_{overhead}, K_{biject}$
Риски	Снижение стойкости, нарушение корректности	Чрезмерный рост вычислительной нагрузки	Нарушение биективности, потеря корректности
Верификация	Сравнение с базовой схемой Kyber	Оценка стойкости LWE	Тестирование на корректность протокола
Область применения	Высокопроизводительные системы	Критически важные системы	Защита от специализированных атак

VI. Заключение

Проведенное исследование позволило разработать и систематизировать комплекс методик совершенствование процесса анализа и параметрического выбора постквантового шифрования, основанных на математических решетках. Как следует из представленной сводной таблицы (табл. 1), каждая из трех предложенных методик решает конкретную задачу модернизации криптографических схем, таких как CRYSTALS-Kyber, и обладает четким облачением применения.

Первая методика, направленная на модификацию алгебраического идеала, позволяет целенаправленно повышать эффективность вычислений без неизбежного перехода на более мощное аппаратное обеспечение.

Вторая методика предлагает системный подход к управлению размерностью, что дает разработчикам инструмент для прогнозируемого увеличения криптографической стойкости, хотя и требует тщательного балансирования с производительностью.

Третья методика вводит новый класс оптимизаций через контролируемое нарушение линейности, открывая пути для создания схем, устойчивых к специализированным алгебраическим атакам.

Важнейшим результатом работы является не только разработка каждой методики в отдельности, но и их интеграция в единый комплекс. Как наглядно демонстрирует сравнительная таблица, эти подходы охватывают ключевые аспекты совершенствования криптографических примитивов: производительность, стойкость и устойчивость к узконаправленным угрозам. Предложенные формализованные критерии верификации и четкие последовательности действий делают методики практическим инструментом для исследователей и инженеров.

Таким образом, комплекс методик создает основу для целенаправленной и обоснованной модернизации перспективных криптографических стандартов, позволяя адаптировать их к постоянно ужесточающимся требованиям по производительности и безопасности в условиях постквантового перехода.

Следует отметить, что представленный комплекс методик носит формально-методологический характер. Разработанные системы коэффициентов и критериев оценки предназначены для использования в последующих прикладных исследованиях, предполагающих численную реализацию предложенных модификаций. В настоящей работе акцент сделан на универсальности и полноте описания методик, а не на их экспериментальной верификации, что составляет направление дальнейших исследований.

Библиография

[1] Ducas L. et al. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme"

[2] National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization. 2022.

[3] Avanzi R., Bos J., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., et al. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation. NIST PQC Round 3 Submission. 2020. 45 p.

[4] Bai S., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., et al. CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. NIST PQC Round 3 Submission. 2021. 63 p.

[5] Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-quantum key exchange—A new hope. USENIX Security Symposium. 2016. Vol. 2016. Pp. 3-24

[6] Bernstein D.J., Lange T. Post-quantum cryptography. Nature. 2017.

Vol. 549. No. 7671. Pp. 188-194.
[7] Langlois A., Stehlé D. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography. 2015. Vol. 75. No. 3. Pp. 565-599.
[8] Zhang J., Zhang Z., Ding J., Snook M., Dagdelen Ö. Authenticated Key Exchange from Ideal Lattices. In: Advances in Cryptology – EUROCRYPT 2015. Springer, 2015. Pp. 719-751.
[9] López-Alt A., Tromer E., Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the 44th annual ACM symposium on Theory of computing. 2012. Pp. 1219-1234
[10] Stehlé D., Steinfeld R. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. In: Advances in Cryptology – EUROCRYPT 2011. Springer, 2011. Pp. 27-47.
[11] Pollard J.M. The fast Fourier transforms in a finite field. Mathematics of Computation, 1971, 25(114): 365-374.
[12] Boneh D., Gentry C., Gorbunov S., Halevi S., Nikolaenko V., Segev G., et al. Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits. In: Advances in Cryptology – EUROCRYPT 2014. Springer, 2014. Pp. 533-556.

Статья получена: 22.12.2025
Н.А.Клейменов –аспирант ПГУПС (email: bark823@gmail.com).
К.З. Билятдинов – д.т.н., профессор ГУАП (email: k74b@mail.ru).

A complex of methods for the improvement of post-quantum encryption algorithms based on the mathematical lattice theory

N.A. Kleymenov, K.Z. Biliatdinov

Abstract - methodological solutions for improving lattice-based post-quantum encryption algorithms are presented. A set of interconnected optimization techniques is proposed, aimed at enhancing the performance and cryptographic strength of cryptographic primitives.

The complex of techniques formalizes the process of improving the algebraic structure underlying modern standards such as CRYSTALS-Kyber. The framework comprises three targeted methodologies: modification of the algebraic ideal to accelerate computations, management of matrix dimensions to enhance security, and introduction of nonlinear distortions to counter specialized attacks. Each methodology includes a formalized sequence of actions, a system of verifiable performance indicators, and clear criteria for evaluating optimization results.

Key words — cryptography, post-quantum cryptography, mathematical lattices, keys, encryption.

REFERENCES

[1] Ducas L. et al. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme"

[2] National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization. 2022.

[3] Avanzi R., Bos J., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., et al. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation. NIST PQC Round 3 Submission. 2020. 45 p.

[4] Bai S., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., et al. CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. NIST PQC Round 3 Submission. 2021. 63 p.

[5] Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-quantum key exchange—A new hope. USENIX Security Symposium. 2016. Vol. 2016. Pp. 3-24

[6] Bernstein D.J., Lange T. Post-quantum cryptography. Nature. 2017. Vol. 549. No. 7671. Pp. 188-194.

[7] Langlois A., Stehlé D. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography. 2015. Vol. 75. No. 3. Pp. 565-599.

[8] Zhang J., Zhang Z., Ding J., Snook M., Dagdelen Ö. Authenticated Key Exchange from Ideal Lattices. In: Advances in Cryptology – EUROCRYPT 2015. Springer, 2015. Pp. 719-751.

[9] López-Alt A., Tromer E., Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the 44th annual ACM symposium on Theory of computing. 2012. Pp. 1219-1234

[10] Stehlé D., Steinfeld R. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. In: Advances in Cryptology – EUROCRYPT 2011. Springer, 2011. Pp. 27-47.

[11] Pollard J.M. The fast Fourier transforms in a finite field. Mathematics of Computation, 1971, 25(114): 365-374.

[12] Boneh D., Gentry C., Gorbunov S., Halevi S., Nikolaenko V., Segev G., et al. Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits. In: Advances in Cryptology – EUROCRYPT 2014. Springer, 2014. Pp. 533-556