Принципы и модель совершенствования алгоритмов постквантового шифрования, основанных на математической теории решёток

Н.А. Клейменов, К.З. Билятдинов

***Аннотация* — представлены принципы, как основа модели совершенствования алгоритмов и направленные на повышение эффективности анализа алгоритмов постквантового шифрования, основанных на математической теории решеток.**

Модель предназначена для систематизации и улучшения процесса совершенствования алгоритмов шифрования на решетках. Применение модели решает проблему оптимального баланса между криптографической стойкостью и практической эффективностью (размерами ключей, скоростью работы, потреблением памяти) при совершенствовании алгоритмов, основанных на математической теории решеток.

В модели реализован подход к совершенствованию анализа постквантовых алгоритмов шифрования на основе принципов параметрической оптимизации, модульности и минимизации данных.

Основной положительный эффект: существенное повышение эффективности анализа криптографических алгоритмов за счёт перехода от описательного анализа к целевой оптимизации по чётко определённым критериям (размер ключа, скорость работы) при гарантированном уровне стойкости.

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

I. Введение

В перспективе развитие квантовых вычислений обусловливает необходимость поиска и реализации новых направлений в области обеспечения информационной безопасности [1]. Сегодня одним из наиболее востребованных направлений защиты информации является криптография. При этом современные криптографические стандарты уязвимы перед атаками с использованием квантовых вычислений. Перспективным решением этой проблемы становятся алгоритмы постквантового шифрования [2], основанные на математической теории решёток (далее – Алгоритмы). Они обеспечивают защиту как от классических, так и от квантовых атак, и благодаря этому их всё чаще начинают использовать в современных компьютерных сетях.

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

Несмотря на преимущества, Алгоритмы имеют и недостатки. Основной недостаток Алгоритмов: большой размер ключей, что затрудняет применение Алгоритмов в системах, где критически важны высокая скорость работы и низкое потребление ресурсов, например, в высоконагруженных сервисах или в устройствах интернета вещей [3].

Поэтому актуальность темы настоящего исследования будет в первую очередь находиться в предметной области совершенствования алгоритмов постквантового шифрования, основанных на математической теории решеток. Проблема размерности ключей создает существенное препятствие применению постквантового шифрования в различных системах. Таким образом, сегодня существует необходимость поиска рациональных решений актуальной задачи модернизации алгоритмов постквантового шифрования.

II. Основы исследования и постановка задачи

Актуальность совершенствования алгоритмов постквантового шифрования предопределяют необходимость применения системного подхода к анализу результатов научных исследований [4, 5, 6], которые потенциально могут быть полезны для модернизации исследуемых Алгоритмов.

Кроме того, с точки зрения системного подхода важно выявить и формализовать взаимосвязи между криптографическими параметрами решёток, безопасностью и длиной ключей.

Вышеизложенное подтверждает потенциальные возможности эффективного использования современных научных достижений при совершенствовании алгоритмов постквантового шифрования основанных на математической теории решеток.

Отсюда целесообразно сформулировать три взаимосвязанные задачи исследования:

1. Определить и систематизировать основные принципы, составляющие основу для совершенствования Алгоритмов.

2. На основе данных принципов разработать модель совершенствования Алгоритмов (далее – Модель) на основе систематизации процесса анализа и оптимизации Алгоритмов. Применение Модели должно быть направлено на рациональное решение задачи уменьшения размеров ключей и повышения

производительности шифров.

3. Состав и содержание принципов и Модели должны обеспечивать их практическую применимость для разработчиков криптографических решений и их дальнейшую реализацию в современных системах защиты информации.

III. Принципы совершенствования Алгоритмов

В рамках разработки Модели были формализованы три взаимосвязанных принципа, составляющие основу для системного повышения эффективности анализа криптографических алгоритмов.

Принципы применимы для формирования единого методологического базиса, позволяющего перейти от частных эмпирических улучшений к целостному и структурированному процессу совершенствования Алгоритмов.

1. Принцип параметрической оптимизации представляет собой систематический подход к целенаправленному подбору и корректировке математических параметров решётки для достижения оптимального баланса между криптографической стойкостью и вычислительной эффективностью. Данный принцип предполагает всесторонний анализ чувствительности стойкости Алгоритма к вариации ключевых параметров без ухудшения параметров безопасности [7], включая размерность решётки, модуль и другие математические характеристики [8].

2. Принцип модульности предполагает структурную декомпозицию Алгоритма на независимые функциональные блоки, что позволяет проводить точечную оптимизацию отдельных компонентов без нарушения общей архитектурной целостности системы. Преимущество модульного подхода заключается в возможности независимой оптимизации каждого компонента с последующей интеграцией улучшенных версий в общую систему. Это существенно упрощает процесс верификации корректности внесённых изменений и обеспечивает возможность повторного использования оптимизированных компонентов в различных алгоритмах. Кроме того, принцип модульности обеспечивает необходимую гибкость при адаптации криптографических алгоритмов к различным аппаратным платформам и вычислительным средам [9].

3. Принцип минимизации данных направлен на сокращение объёмов всех видов криптографических данных — включая ключи, шифротексты и цифровые подписи — без снижения гарантированного уровня криптографической стойкости [10]. Важным аспектом реализации принципа минимизации данных является соблюдение строгих ограничений, включая безусловное сохранение криптографической стойкости, обеспечение обратной совместимости с существующими стандартами и сохранение возможности эффективной верификации корректности криптографических операций [11].

Таким образом, сформулированные принципы способствуют созданию единой системы криптографической защиты информации, в которой параметрическая оптимизация задаёт математическую основу для преобразований, модульность обеспечивает необходимую архитектурную гибкость, а минимизация данных определяет целевые показатели эффективности.

Комплексная реализация всех трёх принципов позволяет проводить системное совершенствование, повышать производительность и эффективности Алгоритмов при гарантированном сохранении требуемого уровня криптографической стойкости.

Такой подход создаёт теоретический фундамент для разработки Модели и её успешной адаптации к требованиям современных информационных систем.

IV. Модель совершенствования Алгоритмов

4.1. Назначение, ограничения и допущения Модели.

Результаты современных научных исследований [1, 4, 7, 11] дают возможность разработки Модели путем унификации и применения системного подхода к оценке параметров Алгоритмов.

Таким образом, предлагаемая Модель представляет собой формализованное описание процесса оптимизации Алгоритмов на основе системы принципов параметрической оптимизации, модульности и минимизации данных.

По результатам исследования и внедрения Модели составлены таблицы сравнительного анализа параметров Алгоритмов (до оптимизации) (табл. 2) и оценки соответствия Алгоритмов критериям устойчивости после оптимизации (табл. 3).

Назначение Модели (рис., табл. 1, 2 и 3):

1. Анализ параметров Алгоритмов и подбор оптимальных значений, которые обеспечивают выполнение требований по безопасности и скорости.

2. Структуризация процесса совершенствование анализа и параметрического выбора постквантового шифрования, основанных на математической теории решеток.

Ограничения при применении Модели:

1. Модель применима для анализа алгоритмов постквантовой криптографии, которые в основе своей используют такие задачи как (LWE, RLWE, NTRU) [12,13,14] и для которых могут быть определены количественные метрики стойкости и эффективности.

2. Модель предполагает, что анализируемый Алгоритм может быть декомпозирован на составные модули (Рис. 1.).

3. Для корректного сравнения эффективности алгоритмов или совершенствования в рамках Модели, должен приводиться анализ на эталонных наборах данных и при одинаковых целевых уровнях стойкости описанным NIST [15].

4. Модель фокусируется на улучшении конкретных, алгоритмических и математических аспектов (размер ключей, сложность операций) и не рассматривает конкретный архитектурные и аппаратные реализации.

Допущения:

1. В качестве базового состояния Алгоритма принимается его эталонная версия с известными исходными показателями стойкости и производительности. (табл. 2).

2. В Модели рассматриваются параметры Алгоритма, изменение которых напрямую влияет на целевые метрики (размер ключей, скорость работы), такие как

размерность решётки, модуль).

3. Для обеспечения оценки стойкости при совершенствовании Алгоритмов рассматривается наихудший сценарий, что позволяет учитывать потенциальные проблемы в методах анализа решётчатых алгоритмов.

4.2. Сущность и краткое содержание Модели.

Модель позволяет оценивать и направленно улучшать основные показатели качества Алгоритмов на основе анализа взаимосвязи между их параметрами, принципами построения и итоговыми характеристиками.

Для этого Модель включает в себя совокупность:

1. Формализованных принципов (параметрическая оптимизация, модульность, минимизация данных).

2. Процедур анализа исходного состояния Алгоритма.

3. Механизмов совершенствования Алгоритма на основе выявленных зависимостей.

4. Методов верификации сохранения требуемого уровня стойкости после оптимизации.

Схема Модели (рис. 1) представлена в виде сети Петри [16], с помощью которой можно описать состояние процесса совершенствования модели на каждом этапе. Модель состоит из событий T и состояний P где:

P1 – получение входных параметров
P2 – анализ принципов
P3 – подтверждение криптостойкости
P4 – требуется модификация
P5 – балансировка
P6 – готовность к проверке
P7 – совершенствование успешно завершено
P8 – ошибка совершенствования
P9 – новая версия алгоритма
T1 – анализ
T2 – балансировка
T3 – модификация
T4 – балансировать
T5 – верификация
T6 – исправить
T7 – повторить

На основании полученной схемы была построена матрица инцидентности (табл. 1). Сеть была проверена на отсутствие тупиковых состояний и на работу обратных связей.

Начальная маркировка сети:

$$M_{0=}[1,0,0,0,0,0,0,0]$$

Из нее можно достичь

$$M_{1=}[1,0,0,0,0,0,0,0]$$
$$M_{2=}[0,0,1,0,0,0,0,0]$$
$$M_{3=}[0,0,0,1,0,0,0,0]$$
$$M_{7=}[0,0,0,0,0,0,1,0]$$
$$M_{8=}[0,0,0,1,0,0,0,0]$$

Что подтверждает отсутствия в ней состояния блокировок и работоспособность обратных переходов.

В качестве двух основных критериев обеспечения устойчивости, которые носят прикладной и эвристический характер предлагаются:

1. Максимально допустимый размер ключей K_{max}.

Если $K \le K_{max}$ $K \le K_{max}$, то алгоритм соответствует целевым требованиям по эффективности; если $K > K_{max}$, то алгоритм требует дальнейшей оптимизации.

2. Минимально допустимая скорость работы V_{min}.

Если $V \ge V_{min}$, то алгоритм соответствует целевым требованиям по производительности; если $V < V_{min}$, то алгоритм требует дальнейшей оптимизации.

Другие принимаемые критерии (объём шифротекста, использование памяти) должны отражать специфику целевой области применения алгоритма.

В Модели основная величина, характеризующая эффективность оптимизации – это коэффициент улучшения (IR), показывающий, во сколько раз целевой показатель был улучшен относительно исходного состояния алгоритма при сохранении уровня стойкости:

$$IR = P_{base}/P_{optimized}$$

где P_{base} – значение показателя (например, размер ключа) до оптимизации, а $P_{asoptimizede}$ – после оптимизации (табл. 3).

Таким образом, $IR > 1$ можно обоснованно считать основным количественным показателем успешности применения Модели для сравнительного анализа и совершенствования алгоритмов.

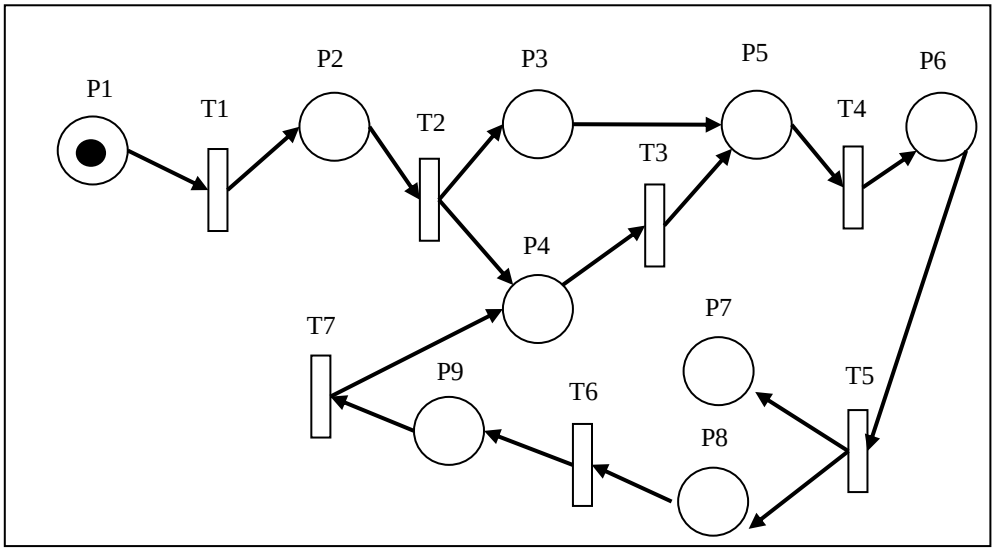

Рис. 1 – Схема модели совершенствования алгоритмов постквантового шифрования,

основанных на математической теории решёток (представлена в виде сети Петри)

Таблица 1

Матрица инцидентности

	T1	T2	T3	T4	T5	T6	T7
P1	-1	0	0	0	0	0	0
P2	+1	-1	0	0	0	0	0
P3	0	-1	0	0	0	0	0
P4	0	-1	-1	0	0	0	+1
P5	0	+1	+1	-1	0	0	0
P6	0	0	0	+1	-1	0	0
P7	0	0	0	0	-1	0	0
P8	0	0	0	0	-1	0	0
P9	0	0	0	0	0	+1	-1

Таблица 2

Сравнительный анализ параметров Алгоритмов до внедрения Модели

№ п/п	Алгоритм	Размер открытого ключа(байт)	Размер секретного ключа(байт)	Уровень стойкости (NIST)	Скорость работы, (операций/сек)
1	Kyber-512	800	1,632	1	1150
2	NTRU-HPS	699	935	1	980
3	Dilithium-2 (подпись)	1,312	2,528	1	850
4	Falcon-512 (подпись)	897	1,281	1	720
5	Saber	672	1,568	1	1050

Таблица 3

Оценка Алгоритмов критериям устойчивости после внедрения Модели

№ п/п	Алгоритм	Исходное состояние (до оптимизации)	Конечное состояние (после оптимизации)	Оценка соответствия критериям устойчивости
1	Kyber-512	K = 1600 байт V = 900 оп/сек	K = 1400 байт V = 1150 оп/сек	Если $K \leq K_{max}$ (1500), то критерий выполнен. Если $V \geq V_{min}$ (1000 оп/сек), то критерий выполнен. Результат критериям соответствует.
2	NTRU-HPS	K = 1800 байт V = 850 оп/сек	K = 1550 байт V = 1010 оп/сек	Если $K \leq K_{max}$ (1500), то критерий выполнен. Если $V \geq V_{min}$ (1000 оп/сек), то критерий выполнен. Результат не соответствует (по скорости).
3	Dilithium-2 (подпись)	K = 1700 байт V = 950 оп/сек	K = 1450 байт V = 1300 оп/сек	Если $K \leq K_{max}$ (1500), то критерий выполнен. Если $V \geq V_{min}$ (1000 оп/сек), то критерий выполнен. Результат критериям соответствует.
4	Falcon-512 (подпись)	K = 1900 байт V = 800 оп/сек	K = 1750 байт V = 900 оп/сек	Если $K \leq K_{max}$ (1500), то критерий выполнен. Если $V \geq V_{min}$ (1000 оп/сек), то критерий выполнен. Результат не соответствует (по обоим критериям).

VI. Заключение

Принципы и Модель, могут быть использованы для совершенствования процесса анализа и параметрического выбора постквантового шифрования, основанных на математической теории решеток.

В ближайшей перспективе (горизонт прогнозирования до 5-7 лет и при условии сохранения существующей динамики развития квантовых компьютеров) применение принципов и Модели обеспечит объективный анализ влияния качества модифицированных решетчатых алгоритмов.

Другое перспективное направление данной статьи — это обеспечение безопасного и устойчивого функционирования компьютерных сетей и информационных систем за счёт сравнительного анализа и целенаправленной оптимизации Алгоритмов, обеспечивая их соответствие современным требованиям по производительности и размеру ключей шифрования.

В этом отношении будет наиболее рационально обеспечиваться достижение целей устойчивого развития защищенных информационных систем в условиях перехода к постквантовой криптографии.

Результаты исследования будут особенно востребованы в системах, функционирующих в условиях ограниченных ресурсов, таких как высоконагруженные сервисы и устройства интернета вещей, где предъявляются повышенные требования к производительности и размеру криптографических данных.

Таким образом, основной положительный эффект от применения разработанных принципов и Модели заключается в существенном сокращении вычислительной нагрузки и объема передаваемых Алгоритмов, а также в систематизации процесса их анализа и оптимизации для достижения целевых показателей эффективности.

Библиография

[1] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 1997. Vol. 26. No. 5. Pp. 304-328.

[2] Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography. NIST IR 8105. 2016.

[3] D'Anvers J.P., Karmakar A., Sinha Roy S., Vercauteren F. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. International Conference on Cryptology in Africa. 2018. Pp 282-305.

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

[5] D'Anvers J.P., Karmakar A., Sinha Roy S., Vercauteren F. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. International Conference on Cryptology in Africa. 2018. Pp. 3-20.

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

[7] Ducas L., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. Vol. 2018. No. 1. Pp. 2–31.

[8] Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. Journal of the ACM. 2013. Vol. 60. No. 6. Pp. 2-31.

[9] Güneysu T., Oder T., Pöppelmann T., Schwabe P. Software Speed Records for Lattice-Based Signatures. In: Cryptographic Hardware and Embedded Systems – CHES 2012. Springer. 2012. Pp. 67-82.

[10] Melchor C.A., Aragon N., Bettaieb S., Bidoux L., Blazy O., Deneuville J.-C., Gaborit P., Zémor G. Hamming Quasi-Cyclic (HQC). NIST PQC Round 3 Submission. 2020.

[11] Avanzi R., Bos J., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schanck J.M., Schwabe P., Seiler G., Stehlé D. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation. NIST PQC Round 3 Submission. 2020.

[12] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. Journal of the ACM. 2009. Vol. 56. No. 6. Pp. 2–35.

[13] Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. Journal of the ACM. 2013. Vol. 60. No. 6. Pp. 2–31.

[14] Hoffstein J., Pipher J., Silverman J.H. NTRU: A Ring-Based Public Key Cryptosystem. In: International Algorithmic Number Theory Symposium (ANTS). Springer. 1998. Pp. 267–288.

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

[16] David R., Alla H. Petri nets for modeling of dynamic systems: A survey // Automatica. – 1994. – Vol. 30. – No. 2. – P. 175–202

Principles and model for improving post-quantum encryption algorithms based on mathematical lattice theory

N.A. Kleimenov, K.Z. Bilyatdinov

Abstract - This paper presents principles that serve as the foundation for a model designed to improve the efficiency of analyzing post-quantum encryption algorithms based on mathematical lattice theory.

The model is intended to systematize and enhance the process of improving lattice-based encryption algorithms. Its application addresses the problem of achieving an optimal balance between cryptographic strength and practical efficiency (key sizes, operational speed, memory consumption) when enhancing algorithms based on mathematical lattice theory.

The model implements an approach to improving the analysis of post-quantum encryption algorithms, based on the principles of parametric optimization, modularity, and data minimization.

The main positive effect is a significant increase in the efficiency of cryptographic algorithm analysis by shifting from descriptive analysis to targeted optimization according to clearly defined criteria (key size, operational speed) while maintaining a guaranteed level of security.

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

REFERENCES

[1] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 1997. Vol. 26. No. 5. Pp. 304-328.

[2] Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography. NIST IR 8105. 2016.

[3] D'Anvers J.P., Karmakar A., Sinha Roy S., Vercauteren F. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. International Conference on Cryptology in Africa. 2018. Pp 282-305.

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

[5] D'Anvers J.P., Karmakar A., Sinha Roy S., Vercauteren F. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. International Conference on Cryptology in Africa. 2018. Pp. 3-20.

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

[7] Ducas L., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. Vol. 2018. No. 1. Pp. 2–31.

[8] Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. Journal of the ACM. 2013. Vol. 60. No. 6. Pp. 2-31.

[9] Güneysu T., Oder T., Pöppelmann T., Schwabe P. Software Speed Records for Lattice-Based Signatures. In: Cryptographic Hardware and Embedded Systems – CHES 2012. Springer. 2012. Pp. 67-82.

[10] Melchor C.A., Aragon N., Bettaieb S., Bidoux L., Blazy O., Deneuville J.-C., Gaborit P., Zémor G. Hamming Quasi-Cyclic (HQC). NIST PQC Round 3 Submission. 2020.

[11] Avanzi R., Bos J., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schanck J.M., Schwabe P., Seiler G., Stehlé D. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation. NIST PQC Round 3 Submission. 2020.

[12] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. Journal of the ACM. 2009. Vol. 56. No. 6. Pp. 2–35.

[13] Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. Journal of the ACM. 2013. Vol. 60. No. 6. Pp. 2–31.

[14] Hoffstein J., Pipher J., Silverman J.H. NTRU: A Ring-Based Public Key Cryptosystem. In: International Algorithmic Number Theory Symposium (ANTS). Springer. 1998. Pp. 267–288.

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

[16] David R., Alla H. Petri nets for modeling of dynamic systems: A survey // Automatica. – 1994. – Vol. 30. – No. 2. – P. 175–202.