УДК 004.056

В.Г. ИВАНЕНКО[1], И.Д. ИВАНОВА[2]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Российский университет транспорта (МИИТ), Москва*

ОПЕРАЦИИ ПО МОДУЛЮ В ПОСТКВАНТОВЫХ СХЕМАХ ПОДПИСИ

Цель исследования: ускорение вычислений над полиномами в постквантовых криптографических системах. Проведен сравнительный анализ алгоритмов приведения чисел по модулю и обоснована применимость алгоритма K-RED в составе постквантовой схемы подписи Falcon. В результате предложен метод ускорения операций генерации ключей и проверки подписей путем синтеза быстрых алгоритмов вычисления числового теоретического преобразования и алгоритма K-RED.

В постквантовой схеме подписи Falcon для создания подписей применяются операции над полиномами в факторкольце, в том числе ресурсоемкое умножение. Для упрощения вычислений может применяться числовое теоретическое преобразование (NTT), в ходе которого коэффициенты преобразованного полинома вычисляются по формуле (1):

$$\tilde{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \; mod \; q, \tag{1}$$

где a – вектор, выражающий исходный полином, q – модуль, по которому производятся вычисления в факторкольце, ω – примитивный корень единицы степени n (по числу коэффициентов полинома).

Для осуществления умножения полиномов используется свойство NTT, выражаемое формулой (2):

$$c = INTT\big(NTT(a) \circ NTT(b)\big), \tag{2}$$

где $INTT$ – обратное преобразование NTT, а $\circ$ – покомпонентное умножение векторов.

Сложность прямого вычисления отрицательно завернутой свертки при помощи NTT составляет $O(n^2)$, потому для достижения сложности $O(n \log n)$ применяются алгоритмы Кули-Тьюки и Джентльмена-Санде для прямого и обратного преобразований соответственно. Однако на

практике существует еще одна проблема: операции по модулю могут быть достаточно затратными при больших значениях порядка q и требовать отдельных алгоритмов ускорения [1].

В эталонной реализации Falcon, представленной на конкурсе NIST, для ускорения операций умножения по модулю в составе NTT используется алгоритм приведения Монтгомери. Данный алгоритм требует приведения величин в форму Монтгомери, что на практике является ресурсоемким. Применение алгоритма приведения по модулю K-RED позволяет ускорить выполнение преобразования NTT в 2 раза [2]. При условии, что модуль, применяемый в алгоритме Falcon, имеет вид:

$$q = 12289 = 3 * 2^{12} + 1. \quad (3)$$

приведение чисел по модулю будет осуществляться при фиксированных параметрах $k = 3, m = 12$ в два шага:

1. Входное число c представляется в виде:

$$v = v_0 + 2^m * v_1. \quad (4)$$

2. Алгоритм возвращает:

$$kv_0 - v_1. \quad (5)$$

Для использования алгоритма K-RED необходимо предварительно вычислить массив масштабированных коэффициентов поворота, а также константы, позволяющие уменьшить в 2 раза количество умножений и приведений по модулю в ходе обратного преобразования NTT [3]. Внедрение алгоритма K-RED в схему подписи Falcon позволяет ускорить операции генерации ключей и проверки подписи в схеме подписи Falcon.

Список литературы

1. Mert A. C. et al. Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture // 2019 22nd Euromicro Conference on Digital System Design (DSD). 2019, p. 253-260. DOI:10.1109/DSD.2019.00045.

2. Bisheh-Niasar M., Azarderakhsh R., Mozaffari-Kermani M. High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography // In Proceedings of the IEEE symposium on Computer Arithmetic (ARITH). 2021, p. 94–101. DOI: 10.1109/ARITH51176.2021.00028.

3. Иваненко В.Г., Иванова И.Д., Иванова Н.Д. Вычисления над полиномами в постквантовых схемах подписи // Вопросы кибербезопасности. 2024, № 4(62), с. 65–70. DOI: 10.21681/2311-3456-2024-4-65-70.