ЗАСТОСУВАННЯ ТЕОРЕТИКО-ЧИСЛОВИХ ПЕРЕТВОРЕНЬ У ЗАВДАННЯХ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Івашко А.В., Лунін Д.О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

В останні роки значно зріс інтерес до алгоритмів прискореного перемноження поліномів над кінцевими полями. Пошук таких алгоритмів є особливо актуальним у зв'язку з використанням постквантової криптографії (PQC) – сукупності криптографічних алгоритмів, що забезпечують безпеку при використанні противником квантових комп'ютерівn [1]. Однією з трудомісткої операції у цих алгоритмах є множення в кільцях поліномів, що вимагає $O(n^2)$ операцій.

Теоретико-числове перетворення (ТЧП) дозволяє прискорити множення поліномів, спрощуючи реалізацію алгоритмів постквантової криптографії на основі грат (*lattice-based cryptography*). В даний час стандартизовані алгоритми PQC FIPS 203 (*Crystals-Kyber*), FIPS 204 (*Crystals-Dilithium*) та FIPS 206 (*Falcon*) використовують ТЧП для виконання множення поліномів.

ТЧП послідовності x_i, $i = 0 \ldots N-1$ визначається як:

$$X_k = \sum_{i=0}^{N-1} x_i \cdot g^{ik} (\bmod p), \tag{1}$$

де модуль p і довжина послідовності N не мають спільних співмножників, а g вибирається так, щоб виконувалася умова:

$$g^N = 1 (\bmod\ p). \tag{2}$$

Алгоритм прискореного множення поліномів зводиться до обчислення ТЧП від двох поліномів, поточкового множення коефіцієнтів та зворотного ТЧП. Застосування швидких методів, аналогічних алгоритмам швидкого перетворення Фур'є дозволяє знизити обчислювальну складність до $O(n \cdot \log_2 n)$.

При розробці алгоритмів швидкого множення поліномів виявляється важливим вибір простого модуля, що забезпечує, з одного боку, простоту обчислень у кільцях поліномів, з іншого – наявність швидких алгоритмів. Було здійснено пошук простих модулів чисел виду $(2^a \pm 1) \cdot 2^b - 1$, що допускають нескладну реалізацію ТЧП та виконано оцінку складності апаратної реалізації ТЧП.

Література:

1. A. Satriawan, I. Syafalni, R. Mareta, I. Anshori, W. Shalannanda and A. Barra. Conceptual Review on Number Theoretic Transform and Comprehensive Review on Its Implementations, in IEEE Access, vol. 11, pp. 70288-70316, 2023, doi: 10.1109/ACCESS.2023.3294446.