ДОСЛІДЖЕННЯ МЕТОДІВ ФАКТОРИЗАЦІЇ МНОГОЧЛЕНІВ ТА ЇХ ЗАСТОСУВАННЯ В КРИПТОГРАФІЇ

Самосєєв Євгеній Дмитрович
студент групи МАМм-1-23-1.4.д
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к..ф-м.н., доц.. Жданова Ю.Д.

Факторизація многочленів – одна з центральних задач в алгебрі та теорії чисел, яка має важливе значення як у чистій математиці, так і в прикладних дисциплінах, зокрема в криптографії. Можливість розкласти многочлен на незвідні множники дозволяє розширити теоретичні знання про структуру полів і кілець, забезпечити фундамент для алгоритмів у комп'ютерній алгебрі, а також знайти нові шляхи забезпечення захисту інформації в криптографії [1,2]. У даній роботі ми дослідили різні методи факторизації многочленів, визначили їх особливості та придатність до застосування в криптографічних протоколах, зокрема в умовах сучасних технологічних викликів.

Метою дослідження було поставлено огляд і порівняння різних методів факторизації многочленів та аналіз їх можливостей застосування в криптографії. Виходячи з мети, основними завданнями стали:

- Аналіз класичних і сучасних методів факторизації многочленів.
- Оцінка ефективності та складності різних алгоритмів для факторизації над раціональними числами та скінченними полями.
- Дослідження криптографічних застосувань факторизації, особливо для протоколів з відкритим ключем та квантово-стійких систем.

Многочлени можуть бути розкладені на множники за допомогою різних методів, які поділяються на детерміновані й ймовірнісні. Серед основних методів факторизації можна виділити:

1. Алгоритм Евкліда – використовується для знаходження найбільших спільних дільників многочленів і є основою для багатьох інших алгоритмів факторизації.
2. Алгоритм Берлекемпа – підхід для факторизації многочленів над скінченними полями, який спирається на розклад характеристичного многочлена.
3. Алгоритм Кантора-Цассенгауза – модифікація, яка підвищує швидкість факторизації, використовуючи властивості скінченних полів.
4. Алгоритм Ленстри-Ленстри-Ловаса (LLL) – метод, що дозволяє факторизувати многочлени з раціональними коефіцієнтами за допомогою редукції ґраток.
5. Алгоритм Шора – квантовий алгоритм, здатний факторизувати многочлени й цілі числа значно швидше, ніж класичні методи, що становить загрозу для сучасних криптосистем.

Дослідження цих методів показало, що кожен має свої переваги залежно від типу поля, у якому проводиться факторизація, а також від потреби у швидкості або стійкості до зломів.

Порівняння алгоритмів факторизації вказує на їхню ефективність і складність залежно від обраного підходу. Наприклад, алгоритм LLL є надзвичайно ефективним для многочленів з раціональними коефіцієнтами, а алгоритм Кантора-Цассенгауза більш придатний для факторизації в скінченних полях. Сучасні дослідження показують, що ефективні методи факторизації, такі як LLL та його модифікації, можуть використовуватися для факторизації над скінченними полями, що знижує потребу в квантових обчисленнях.

Факторизація многочленів є основою для багатьох криптографічних систем, включаючи:

1. RSA та криптографія з відкритим ключем. Основу криптографічної системи RSA становить факторизація великих чисел, яка може бути поширена на випадок многочленів. Зокрема, виявлення незвідних многочленів може сприяти розробці стійких схем шифрування [3].

2. Постквантова криптографія. Квантові обчислення, зокрема алгоритм Шора, дозволяють розв'язувати задачі факторизації многочленів значно швидше, що підриває стійкість сучасних криптографічних систем. Тому розглядаються нові алгоритми шифрування, стійкі до квантових атак, які можуть використовувати факторизацію над скінченними полями [4].

3. Криптографія на еліптичних кривих. Тут факторизація многочленів використовується для аналізу дискретного логарифму на еліптичних кривих, що є основою безпеки еліптичних криптосистем [5].

4. Схеми на основі ґраток. Ґраткові криптосистеми, що використовують факторизацію многочленів, розглядаються як перспективний напрям у постквантовій криптографії, оскільки факторизація у ґраткових структурах важко обчислювана навіть для квантових комп'ютерів.

Дослідження показало, що факторизація многочленів є важливою математичною задачею з широким спектром застосувань у криптографії. Методи факторизації багато в чому визначають ефективність і безпеку сучасних криптографічних систем. Удосконалення існуючих алгоритмів і розробка нових методів факторизації, зокрема тих, що використовуються в криптографії з відкритим ключем і постквантовій криптографії [6], дозволить захистити інформацію у швидко змінюваному цифровому світі.

ДЖЕРЕЛА

1. Fan, X., Xu, C., & Zhang, Y. (2020). Efficient Factorization of Polynomials over Finite Fields using Heuristic Approaches. Journal of Symbolic Computation, 99, 45-58.

2. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). Theoretical and practical aspects of the use of mathematical methods and information technology in education and science. https://doi.org/10.28925/9720213284km

3. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка, 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

4. M. Iavich, et al., Classical and post-quantum encryption for GDPR, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 70–78.

5. A. Bessalov, et al., Implementation of the CSIDH algorithm model on supersingular twisted and quadratic Edwards curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

6. Bernstein, D. J., Lange, T. (2017). Post-quantum cryptography. *Nature*, 549, 188-194.