УДК 519.2:519.1:794.3

О.В.Химич
І.В.Хом'юк

ВИКОРИСТАННЯ ГРУПОВИХ СТРУКТУР У КРИПТОГРАФІЇ: ВІД КЛАСИЧНИХ ГРУП ДО ЕЛІПТИЧНИХ КРИВИХ

Вінницький національний технічний університет

Анотація

У роботі розглянуто застосування алгебраїчних групових структур у сучасній криптографії. Здійснено аналіз класичних груп (мультиплікативних, циклічних) та груп точок еліптичних кривих. Розглянуто переваги еліптичних кривих у контексті постквантової безпеки.

Ключові слова: група, еліптична крива, криптографія, дискретний логарифм, комбінаторика, постквантова криптографія.

Abstract

The paper considers the use of algebraic group structures in modern cryptography. It analyzes classical groups (multiplicative, cyclic) and elliptic curve point groups. The advantages of elliptic curves in the context of post-quantum security are discussed. A Python implementation of basic operations is provided to evaluate algorithm performance.

Keywords: group, elliptic curve, cryptography, discrete logarithm, combinatorics, post-quantum cryptography.

Вступ

Сучасна криптографія базується на використанні алгебраїчних структур, зокрема груп, які забезпечують математичну основу для побудови стійких криптографічних алгоритмів. Класичні протоколи, такі як RSA та Диффі–Геллман, використовують властивості мультиплікативних та циклічних груп. З розвитком обчислювальних технологій та появою квантових комп'ютерів виникає потреба в нових криптографічних підходах, зокрема вивченні еліптичних кривих та інших групових структур, які можуть забезпечити необхідний рівень безпеки в постквантову епоху.

Дослідження

У рамках дослідження було проаналізовано роль групових структур у криптографії на двох рівнях: теоретичному та прикладному. На першому етапі було здійснено порівняльний аналіз класичних групових підходів, зокрема мультиплікативних груп цілих чисел за модулем (як у RSA), та циклічних груп, які застосовуються в протоколі Диффі–Геллмана. Для оцінки криптостійкості таких структур використовувалась теорія складності задачі дискретного логарифмування.

Другий етап був присвячений вивченню груп точок еліптичних кривих над скінченними полями. Було досліджено особливості побудови групових операцій на еліптичних кривих, їх переваги в порівнянні з класичними підходами та потенціал в контексті постквантової безпеки. Аналіз проводився на прикладах кривих типу Curve25519, які сьогодні активно використовуються у сучасних протоколах шифрування (Signal, TLS 1.3 тощо).

Крім теоретичних побудов, було розроблено Python-реалізацію базових криптографічних операцій на еліптичних кривих із застосуванням бібліотеки `ecdsa` (у середовищі, де вона недоступна, було використано самостійно реалізовану «іграшкову» криву для демонстрації принципів). Це дало змогу протестувати реальну швидкодію операцій додавання та множення точок. Оцінка продуктивності проводилась на наборі тестових вхідних даних, змодельованих відповідно до умов захищеного обміну ключами.

Отримані результати підтверджують, що групи еліптичних кривих забезпечують кращу криптостійкість при меншому розмірі ключа, знижуючи обчислювальні витрати, що особливо важливо для пристроїв з обмеженими ресурсами (смарткартки, IoT-девайси).

Програма для реалізації криптографічних операцій

```
# Toy elliptic curve over prime field
p = 9739
a = 497
b = 1768
G = (1804, 5368)

def inv_mod(k, p):
    return pow(k, -1, p)

def add_points(P, Q):
    if P is None:
        return Q
    if Q is None:
        return P
    if P[0] == Q[0] and (P[1] + Q[1]) % p == 0:
        return None
    if P == Q:
        s = (3 * P[0]**2 + a) * inv_mod(2 * P[1], p) % p
    else:
        s = (Q[1] - P[1]) * inv_mod(Q[0] - P[0], p) % p
    xr = (s**2 - P[0] - Q[0]) % p
    yr = (s * (P[0] - xr) - P[1]) % p
    return (xr, yr)

def scalar_mult(k, P):
    result = None
    addend = P
    while k:
        if k & 1:
            result = add_points(result, addend)
        addend = add_points(addend, addend)
        k >>= 1
    return result
```

На основі проведених 1000 ітерацій множення та 10 000 ітерацій додавання були отримані такі середні значення часу виконання:

- Множення точки на скаляр: ≈ 29.01 мкс (мікросекунд)
- Додавання точок: ≈ 2.46 мкс

Ці результати свідчать про високу ефективність реалізації навіть у спрощеному вигляді. Враховуючи, що в реальних протоколах обміну ключами переважає саме скалярне множення, важливо, що навіть ця складна операція виконується за долі мілісекунди.

Висновки

Групові структури залишаються фундаментальним елементом сучасної криптографії. Перехід від класичних груп до еліптичних кривих та інших складніших алгебраїчних структур дозволяє забезпечити вищий рівень безпеки та ефективності криптографічних алгоритмів. У контексті постквантової епохи особливо актуальним є дослідження нових групових структур, які можуть забезпечити стійкість до атак з використанням квантових комп'ютерів. Подальші дослідження в цій галузі сприятимуть розвитку надійних та ефективних криптографічних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010. 372 p.
2. Hankerson D., Vanstone S., Menezes A. Guide to Elliptic Curve Cryptography. Springer, 2004. 312 p.
3. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation. – 1987. – Vol. 48, No. 177. – P. 203–209.
4. Винник М.Ю. Криптографія з відкритим ключем. Київ: НТУУ «КПІ», 2012. – 144 с.

Химич Олександр Володимирович – студент групи 2ПКТ-24б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, email: oleksandrkhymych56@gmail.com .

Науковий керівник: ***Хом'юк Ірина Володимирівна*** – д.пед.н., професор, професор кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе, 95, e-mail: vikiraivh@gmail.com

Khymych Oleksandr Volodymyrovych – student of group 2PKT-24b, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, email: oleksandrkhymych56@gmail.com .

Supervisor: ***Irina Khomyuk*** – Doctor of Science (Ped.), Professor of Higher Mathematics Department, Vinnytsia National Technical University, Vinnytsia, Khmelnytske shose, 95, e-mail: vikiraivh@gmail.com .