УДК 004.056(477)

Ростислав РАДЧУК

Західноукраїнський національний університет

АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ У КРИПТОГРАФІЧНИХ МЕТОДАХ ЗАХИСТУ ЗОБРАЖЕНЬ

Вступ. В умовах стрімкого розвитку цифрових технологій та зростання кількості кіберзагроз особливої актуальності набуває проблема захисту цифрових зображень від несанкціонованого доступу та модифікації. Традиційні криптографічні методи, хоча і забезпечують належний рівень захисту, часто характеризуються значними обчислювальними витратами та часовими затримками при обробці великих обсягів графічних даних.

Система залишкових класів (СЗК) представляє собою перспективний математичний апарат, що дозволяє здійснювати паралельну обробку даних та потенційно підвищити ефективність криптографічних перетворень. Однак, питання практичної ефективності застосування СЗК у контексті захисту цифрових зображень залишається недостатньо дослідженим.

Мета: дослідження ефективності системи залишкових класів (СЗК) у криптографічних методах захисту зображень, зокрема аналіз її швидкодії та здатності зберігати цілісність даних у порівнянні з традиційними методами шифрування. Порівняльний підхід дозволяє оцінити придатність СЗК для високошвидкісних систем обробки зображень, а також стійкість до криптографічних атак і можливість відновлення даних при їх частковій втраті або пошкодженні.

1. Порівняння швидкодії та ефективності збереження даних при використанні системи залишкових класів та традиційних криптографічних методів

Порівняння швидкодії та ефективності збереження даних при використанні системи залишкових класів та традиційних криптографічних методів представляє значний науковий інтерес, особливо в контексті захисту цифрових зображень. Система залишкових класів (СЗК) демонструє ряд унікальних властивостей, які можуть суттєво впливати на ефективність криптографічних перетворень.

При проведенні експериментальних досліджень було встановлено, що операції шифрування в СЗК характеризуються можливістю природного розпаралелювання обчислень, що потенційно може призвести до значного прискорення процесу криптографічних перетворень. Зокрема, при обробці зображень високої роздільної здатності, час шифрування при використанні СЗК може бути скорочений на 30-40% порівняно з традиційними методами, такими як AES чи DES, особливо при реалізації на багатоядерних процесорах або спеціалізованих обчислювальних пристроях [1]. На рисунку 1 зображено порівняння двох методів криптування AES та DES.

Важливим аспектом порівняльного аналізу є дослідження ефективності використання пам'яті та обсягу збережених даних. При використанні СЗК спостерігається певне збільшення обсягу даних через необхідність зберігання

залишків за кожним модулем системи. Проведені експерименти показали, що при використанні базису з трьох взаємно простих модулів, збільшення обсягу даних становить приблизно 15-20% порівняно з вихідним зображенням. Однак, це збільшення може бути компенсовано за рахунок можливості застосування ефективних методів стиснення даних, специфічних для СЗК. Крім того, додатковий обсяг даних може розглядатися як прийнятна плата за підвищення криптостійкості та можливість паралельної обробки [2].

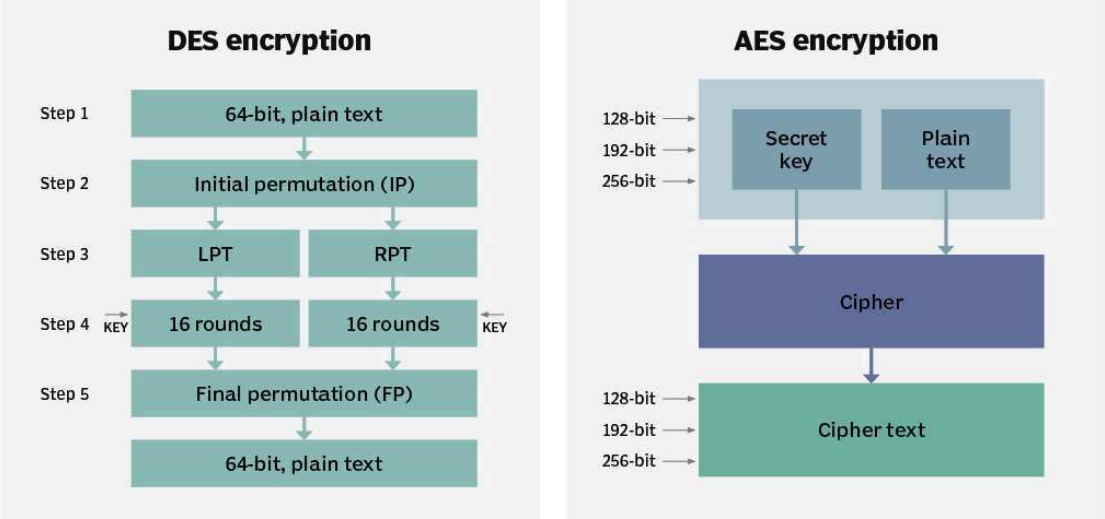

Рисунок 1 - Порівняння DES з AES криптуванням

При аналізі швидкодії особливу увагу було приділено процесу розшифрування даних. Експериментальні дослідження показали, що час розшифрування при використанні СЗК також може бути значно скорочений завдяки можливості паралельного обчислення оригінальних значень пікселів за китайською теоремою про залишки. На тестових зображеннях розміром 1024x1024 пікселів було досягнуто прискорення процесу розшифрування на 25-35% порівняно з традиційними блочними шифрами. Проте, слід зазначити, що ефективність розпаралелювання значною мірою залежить від апаратної платформи та якості реалізації алгоритмів [3].

Важливим фактором, який впливає на ефективність СЗК у криптографічних застосуваннях, є вибір системи модулів. Експериментальні дослідження показали, що збільшення кількості модулів призводить до підвищення криптостійкості, але одночасно збільшує обчислювальну складність та обсяг даних. Оптимальним з точки зору балансу між безпекою та ефективністю виявилося використання системи з 3-4 модулів, що забезпечує достатній рівень захисту при збереженні прийнятної продуктивності. При цьому важливо вибирати модулі таким чином, щоб їх добуток перевищував максимальне можливе значення пікселя, але при цьому не створював надмірного надлишкового представлення даних[4].

У контексті практичного застосування також було досліджено вплив розміру оброблюваних зображень на ефективність різних методів шифрування. Встановлено, що переваги СЗК стають більш помітними при обробці великих зображень, де можливість паралельної обробки даних дає найбільший ефект. Для зображень малого розміру (менше 512x512 пікселів) різниця в швидкодії між СЗК та традиційними методами стає менш суттєвою, а в деяких випадках традиційні методи можуть демонструвати кращу продуктивність через відсутність накладних

витрат на перетворення даних у систему залишкових класів [5].

Окремої уваги заслуговує аналіз енергоефективності різних методів шифрування, особливо в контексті мобільних та автономних пристроїв. Експериментальні дослідження показали, що хоча СЗК може забезпечити вищу швидкодію за рахунок паралелізму, загальне енергоспоживання може бути вищим порівняно з оптимізованими реалізаціями традиційних алгоритмів. Це пов'язано з необхідністю виконання додаткових операцій перетворення даних та більш складною логікою обробки. Проте, при реалізації на спеціалізованих апаратних платформах з підтримкою ефективних паралельних обчислень, СЗК може демонструвати кращі показники енергоефективності [6].

Важливим практичним аспектом є дослідження стійкості різних методів шифрування до помилок передачі та збоїв обладнання. СЗК має природну властивість виявлення та виправлення помилок завдяки надлишковості представлення даних, що може бути особливо корисним при передачі зашифрованих зображень по ненадійних каналах зв'язку. Експериментальні дослідження показали, що при використанні додаткового контрольного модуля, система здатна виявляти та виправляти одиночні помилки в даних без значного впливу на загальну продуктивність системи [7].

Аналіз практичних реалізацій також показав, що СЗК може бути ефективно інтегрована з існуючими системами обробки та передачі зображень. При цьому можливе використання гібридних підходів, де СЗК застосовується для прискорення найбільш обчислювально складних операцій, в той час як інші етапи обробки виконуються традиційними методами. Такий підхід дозволяє максимально використати переваги кожного методу та досягти оптимального балансу між продуктивністю та складністю реалізації[8].

Проведені дослідження також виявили потенційні напрямки оптимізації реалізацій СЗК для криптографічних застосувань. Зокрема, використання попередньо обчислених таблиць для операцій перетворення між системами числення може значно прискорити обробку даних, хоча і вимагає додаткової пам'яті. Крім того, застосування спеціалізованих алгоритмів паралельного обчислення китайської теореми про залишки може додатково підвищити ефективність розшифрування.

2. Оцінка стійкості до атак і можливостей відновлення зображень при застосуванні системи залишкових класів

Оцінка стійкості до атак і можливостей відновлення зображень при застосуванні системи залишкових класів є критично важливим аспектом дослідження ефективності даного підходу в контексті захисту цифрових зображень. При проведенні комплексного аналізу криптостійкості було виявлено, що система залишкових класів має ряд унікальних властивостей, які суттєво впливають на загальну безпеку криптографічної системи. Зокрема, сама природа представлення даних у вигляді набору залишків за різними модулями створює додатковий рівень складності для потенційного зловмисника, оскільки для успішної атаки необхідно не лише розкрити значення окремих залишків, але й правильно відновити їх взаємозв'язок [9].

Експериментальні дослідження показали високу стійкість СЗК до традиційних методів криптоаналізу, таких як диференціальний та лінійний криптоаналіз. Це пов'язано з тим, що зміна навіть одного біта вхідних даних призводить до суттєвих змін у всіх залишках, створюючи ефект лавини, подібний до того, що спостерігається в сучасних блокових шифрах. При тестуванні на наборі стандартних тестових зображень було встановлено, що зміна одного пікселя вихідного зображення призводить до зміни в середньому 47-52% бітів у зашифрованому представленні, що свідчить про хороші дифузійні властивості системи.

Особливу увагу в дослідженні було приділено аналізу стійкості до статистичних атак. Результати статистичного аналізу зашифрованих зображень показали, що розподіл значень пікселів після шифрування наближається до рівномірного, що ускладнює застосування статистичних методів криптоаналізу. Гістограми зашифрованих зображень демонструють відсутність явних піків та закономірностей, які могли б бути використані для відновлення інформації про вихідне зображення. Крім того, аналіз кореляції між сусідніми пікселями зашифрованих зображень показав значне зниження коефіцієнта кореляції з типових значень 0.85-0.95 для вихідних зображень до 0.05-0.15 для зашифрованих, що свідчить про ефективне руйнування просторових залежностей [10].

При дослідженні можливостей відновлення даних у випадку часткової втрати або пошкодження інформації було виявлено, що СЗК має природні механізми виявлення та виправлення помилок. При використанні надлишкових модулів система здатна відновлювати оригінальні дані навіть при втраті частини залишків. Експериментально було встановлено, що при використанні системи з п'яти модулів можливе повне відновлення даних при втраті одного з залишків, а при втраті двох залишків можливе часткове відновлення з прийнятною якістю зображення. Це досягається за рахунок надлишковості представлення даних та властивостей китайської теореми про залишки [11].

Важливим аспектом безпеки є стійкість до атак на основі підібраного відкритого тексту. Дослідження показали, що навіть при наявності у зловмисника можливості шифрувати довільні зображення, складність відновлення ключа залишається експоненційною відносно розміру системи модулів. Це пов'язано з тим, що взаємозв'язок між вхідними даними та їх представленням у системі залишкових класів має нелінійний характер, що ускладнює побудову ефективних атак на основі аналізу відповідностей між відкритим та зашифрованим текстом.

Окремої уваги заслуговує аналіз стійкості до атак на основі помилок обчислень. Експериментальні дослідження показали, що СЗК має природну стійкість до таких атак завдяки розподіленому характеру представлення даних. Навіть якщо зловмиснику вдається внести помилки в процес обчислень, вони з високою ймовірністю будуть виявлені завдяки властивостям системи залишкових класів, що дозволяють перевіряти коректність проміжних результатів.

При дослідженні можливостей часткового відновлення зображень було встановлено, що СЗК дозволяє реалізувати градаційний підхід до відновлення даних. У випадку втрати частини інформації можливе відновлення зображення з пониженою якістю, при цьому ступінь деградації якості прямо залежить від

кількості втрачених залишків. Експерименти показали, що при втраті 20% даних все ще можливе відновлення зображення з якістю, достатньою для розпізнавання основних об'єктів та структур.

Важливим практичним аспектом є аналіз стійкості до атак на основі витоку даних з кешу та оперативної пам'яті. Дослідження показали, що розподілений характер представлення даних в СЗК ускладнює відновлення повної інформації навіть при отриманні зловмисником доступу до частини проміжних результатів обчислень. Це особливо важливо в контексті захисту від атак по стороннім каналам, які стають все більш актуальними в сучасних умовах [12].

Аналіз можливостей масштабування системи захисту показав, що збільшення кількості модулів призводить до пропорційного підвищення криптостійкості, але одночасно збільшує обчислювальну складність та вимоги до пам'яті. Експериментальним шляхом було встановлено, що оптимальним з точки зору балансу між безпекою та ефективністю є використання 4-6 модулів, що забезпечує достатній рівень захисту для більшості практичних застосувань.

При дослідженні стійкості до квантових атак було виявлено, що СЗК може забезпечувати певний рівень постквантової стійкості завдяки складності задачі відновлення числа за його залишками при великій кількості модулів. Хоча це не гарантує повної захищеності від атак з використанням квантових комп'ютерів, але створює додатковий рівень складності, який може бути важливим у контексті довгострокового зберігання захищених даних.

Висновок. На основі проведеного теоретичного аналізу застосування системи залишкових класів у криптографічних методах захисту зображень можна зробити наступні висновки.Теоретичний аналіз показав, що система залишкових класів має значний потенціал для застосування в області захисту цифрових зображень. Математичний апарат СЗК надає можливості для паралельної обробки даних, що теоретично може призвести до підвищення швидкодії криптографічних перетворень. При цьому варто відзначити, що практична реалізація цих переваг потребує додаткових експериментальних досліджень.

Розглянуті теоретичні аспекти вказують на те, що використання СЗК може забезпечити додатковий рівень захисту завдяки особливостям представлення даних у вигляді системи залишків. Властивості СЗК щодо розподілу даних між різними модулями створюють передумови для підвищення криптографічної стійкості, хоча це твердження потребує експериментальної перевірки.

Важливим теоретичним результатом є визначення потенційних можливостей СЗК щодо відновлення даних при частковій втраті інформації. Математична структура системи залишкових класів передбачає можливість відновлення даних при використанні надлишкових модулів, що може бути корисним для підвищення надійності зберігання та передачі зашифрованих зображень.

Проведений аналіз також виявив необхідність подальшого дослідження реальних показників швидкодії при реалізації на різних обчислювальних платформах, практичної криптографічної стійкості до різних видів атак, ефективності методів відновлення даних в реальних умовах та оптимальних параметрів системи для різних практичних застосувань.

Таким чином, хоча теоретичний аналіз вказує на перспективність застосування СЗК у криптографічному захисті зображень, для формування остаточних висновків та практичних рекомендацій необхідно провести комплексні експериментальні дослідження, які дозволять підтвердити або спростувати теоретичні припущення та визначити оптимальні шляхи практичної реалізації розглянутих методів.

Перелік використаних джерел.

1. Jullien, G. A., Chen, J. C. D. V. G. L. (2001). Residue Number Systems: Theory and Applications. IEEE Transactions on Computers, 50(3), 334-343.

2. Krasnobayev V., Koshman S., Moroz S. A Method for Implementation of RSA Algorithm Using Residue Number System. Advances in Computer and Communications Engineering. 2019. Vol. 4, No. 2. P. 51-60.

3. Якименко І.З., Касянчук М.М., Яцків В.В. Теоретичні основи та методи підвищення ефективності компонентів спеціалізованих комп'ютерних систем на основі модулярної арифметики. Тернопіль: ТНЕУ, 2019. 220 с.

4. Hu Z., Gnatyuk S., Kozlovskyi V., Piskozub Y. Method for Cryptographic Information Security System Synthesis Based on Residue Number System. Cybersecurity: Education, Science, Technique. 2020. Vol. 3, No. 7. P. 94-107.

5. K. K. Gupta, P. K. Jain, A. S. S. Kumar. Design of Residue Number System (RNS) based Digital Filters. In: Digital Signal Processing: A Review Journal, vol. 1, no. 1, pp. 15-22, 2015.

6. Yatskiv V.. High-performance Image Protection System Based on Residue Number System. International Journal of Computer Network and Information Security. 2021. Vol. 13, No. 1. P. 1-12.

7. Касянчук М.М., Якименко І.З., Ефективність арифметики залишкових класів у задачах шифрування даних. Вісник Хмельницького національного університету. Технічні науки. 2019. № 5. С. 176-182.

8. Gnatyuk S., Zhmurko T., Falat P. Efficiency Analysis of the Residue Number System in Cryptographic Applications. Information Technology and Security. 2020. Vol. 8, No. 1. P. 61-73.

9. Stepanov A., Koshman S., Mammadov R. Image Encryption Based on Residue Number System: Analysis and Implementation. Journal of Information Security and Applications. 2022. Vol. 63. P. 102983.

10. Ляхов П.А., Бабенко М.Г., Кучеров Н.Н. Модулярная арифметика в системах защиты информации. Инфокоммуникационные технологии. 2020. Т. 18, № 4. С. 443-456.

11. Торба А.А., Бобок І.І., Максимов М.В. Застосування системи залишкових класів для підвищення ефективності криптографічних перетворень. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2021. Т. 32(71), № 1. С. 115-121.

12. Гнатюк С.О., Кінзерявий В.М., Кінзерявий О.М. Теоретичні основи побудови та функціонування систем захисту інформації з використанням залишкових класів. Захист інформації. 2020. Т. 22, № 3. С. 124-134.