Аналіз стійкості криптосистеми McEliece

Владислав Керничний[1], Олександр Сєвєрінов[1]

1. Кафедра безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки,
УКРАЇНА, г. Харків, пр. Науки, 14,
E-mail: vladyslav.kernychnyi@nure.ua
oleksandr.sievierinov@nure.ua

Коротка анотація – Questions of construction of post-quantum cryptosystems based on algebraic codes are considered. McEliece's robustness to cryptographic attacks is analyzed.

Ключові слова – криптосистема на основі алгебраїчних кодів, криптосистема McEliece, код Goppa, атаки

I. Вступ

На основі сучасних уявлень про квантові комп'ютери існує гіпотеза, що після своєї появи вони будуть здатні зруйнувати більшість, якщо не абсолютно всі традиційні криптосистеми, що широко використовуються на практиці.

На даний момент немає однозначного рішення, щодо вибору кращої постквантової криптосистеми. Існує декілька напрямів, що побудовані на різних алгебраїчних структурах:

– схеми, побудовані на алгебраїчних решітках, мають неясні перспективи зростання рівня безпеки;

– схеми багатовимірної криптографії, побудовані на рішеннях рівнянь, заснованих на багатовимірних поліномах над кінцевим полем, мають такі ж невизначені перспективи криптографічної стійкості для квантового комп'ютера;

– схеми основі хеш-функцій;

– криптосистеми на основі алгебраїчних кодів.

Тому актуальним є дослідження стійкості існуючих криттосистем на основі алгебраїчних кодів, а саме системи McEliece.

II. Криттосистема Mceliece

Перша криптосистема побудована на алгебраїчній теорії кодування була запропонована в 1978 році Робертом МакЕлісом [1]. У запропонованій МакЕлісом початковій конструкції використовуються двійкові коди Goppa [1, 2], але алгоритм може бути використовується з будь-якими лінійними кодами.

Відкритий ключ визначає випадковий бінарний код Гоппа. Зашифрований текст - це кодове слово та випадкові помилки.

Приватний ключ дозволяє досить швидко виконувати наступні дії: витягати кодове слово з зашифрованого тексту, виявляти та видаляти помилки.

Система McEliece була спроектована як одностороння (OW-CPA) - це означає, що зловмисник не може швидко знайти кодове слово з зашифрованого тексту та відкритого ключа, під час випадкової вибірки кодового слова.

На даний час рівень безпеки системи McEliece залишається на досить високому рівні, незважаючи на десятки задокументованих нападів на протязі 40 років. Початкові параметри McEliece були розраховані на 64 біта, але систему легко модифікувати та зробити актуальною при різних ступенях розвитку комп'ютерної техніки, включаючи квантові комп'ютери.

Криптографічна стійкість системи заснована на двох складних обчислювальних завданнях: вичерпному пошуку по ключовому простору і декодуванню по максимуму правдоподібності.

III. Атаки на криптосистему Mceliece

У літературі описана досить велика кількість атак на McEliece [3-5]. Деякі атаки, так звані структурні атаки, засновані на спробі побудувати декодер для коду, згенерованого відкритим ключем G. Якщо така спроба виявиться успішною, то закритий ключ буде розкритий, а криптосистема повністю зламана. Код C*, породжений матрицею G* і код C, породжений матрицею G, належать одному еквівалентному класу. Зловмисник повинен порівняти елементи коду з кожного класу в C* для того, щоб визначити еквівалентний код. Оскільки еквівалентні класи мають дуже малу потужність, цей процес виходить за рамки можливостей навіть найпотужніших комп'ютерів. Для оригінальних параметрів (1024, 524, 50) дана структурна атака вимагає для вивчення більш 2^{466} кодів.

Інші атаки спрямовані на отримання вихідного тексту повідомлення з шифрованого повідомлення. Більшість з них засновані на декодуванні безлічі даних (ISD). Або на парадоксі днів народження, їх узагальненнях і покращеннях.

Існують такі атаки, як, наприклад, ітераційне декодування і статичне декодування, але вони не є успішними. Атака ISD виявилася найменш складною. В останні роки було описано декілька алгоритмів і їх покращенн. Найбільш важливі перераховані у Таблиці 1 разом з їх двійковим показником витрат для декодування (1024, 524, 50) коду Гоппа. Для цих алгоритмів відомі їх граничні показники.

ТАБЛИЦЯ 1

Алгоритми ISD-атак с двійковим показником складності

Рік	Алгоритм	Складність ($\log_2$)
1986	Адамс-Мейер	80,7
1988	Лі-Брікелл	70,89
1989	Штерн	66,21
1994	Кантеаут-Шабант	65,5
1998	Кантеаут-Шабант	64,1
2008	Бернштейн-Ланг-Петерс	60,4
2009	Фінназ-Сендреір	59,9

Найактуальніші атаки використовують інформаційне декодування, або ISD. Найпростіша форма ISD, будується на аналізі інформації про помилки в коді. Інформаційний набір, за визначенням, це набір позицій, який визначає ціле кодове слово. Набір вважається безпомилковим, якщо він уникає всіх помилок в отриманому слові, тобто, в зашифрованому тексті. Зловмисник визначає решту кодового слова за допомогою лінійної алгебри, і перевіряє чи була атака успішною, шляхом перевірки ваги помилки t.

Очікується, що випадковий набір позицій k, буде інформаційним набором з великою вірогідністю. Проте, кількість встановлення безперервно падає зі зростаючою кількістю помилок. Наступне асимптотичне твердження є правильним для будь-якого справжнього числа R в проміжку $0 < R < 1$: якщо розмірність коду $k \in (R + O(1))\times n$, і кількість помилок $t \in \Theta(n/\log_n)$, тоді імовірність того, що набір буде безпомилковим буде дорівнювати $(1 – R + O(1))^e$ та n буде прагнути до нескінченності. Складність ISD є такою $(1/(1\text{-}R) + O(1))^e$ [3-5].

Подальші модернізації ISD вплинули на O(1), але не змінили константу 1/(1-R). В системі McEliece t є асимптотичним $(1 – R + O(1))n/\lg_n$, тому припущення $t \in \Theta(n/\log_n)$ є справедливим. Таким чином рівень безпеки McEliece проти цієї атаки дорівнює $n/\lg_n$ з $1/(1 - R)^{1-R} + O(1)$.

Тим часом розмір шифртексту є $(1 – R + O(1))\times n$ бітів, та розмір ключа дорівнює $(R(1 - R) + O(1))\times n^2$ бітів. Таким чином, рівень безпеки 2^5 використовує ключ розміром $(C_0 + O(1))\times b^2(\lg b)^2$, де $C_0 = R/(1 - R)(\lg(1 - R))^2$. Мінімальне значення, яке може досягти C_0 дорівнює близько 0.7418860694, коли R рівне близько 0.7968121300 [3-6].

Традиційний підхід до атак підібраного шифртексту на систему McEliece – це додавання помилок до зашифрованого тексту Gm + e. Це еквівалентно додаванню помилок до e. Розшифрування виконується тоді і тільки тоді, коли отриманий вектор помилок має вагу t, тобто, точно одна із декількох позицій помилки вже буде в e. Таким чином можливо знайти e.

Але ці напади не спрацовують проти актуальної версії системи McEliece. По-перше, декапсуляція змушує зашифрований текст включати хеш e як підтвердження, а зловмиснику неможливо обчислити хеш модифікованої версії e. По-друге, механізм інкапсуляції ключів не виявляє помилок дешифрування: модифікований шифрований текст буде генерувати непередбачуваний сеансовий ключ, незалежно від того, чи є вбудований вектор помилок вагою t.

Висновки

До сих пір криптосистема McElice з кодами Гоппа не піддається криптоаналізу. Найбільш відомі атаки використовують алгоритм декодування множини даних. В останніх реалізаціях показано як атаки на систему, так і її захист від них. В інших показано, що для квантових обчислень розмір ключа повинен бути збільшений на чотири порядки через удосконалення декодування множини даних. Криптосистема має кілька переваг [7]. Шифрування і дешифрування проходить швидше і з ростом довжини ключа ступінь захисту даних зростає набагато швидше. Довгий час вважалося, що McEliece не може бути використана для ЕЦП. Однак виявилося можливим побудувати схему для ЕЦП (наприклад криптосистема Нідеррайтера).

Недоліком криптосистем McEliece є великий обсяг ключової інформації - від декількох мегабайт. Крім того, вони потребують навіть більших ключів для захисту від квантових комп'ютерів. Через недоліки McEliece використовується рідко. Один з винятків - використання McElice для шифрування в Freenet-подібної мережі ENTROPY.

Література

[1] R. J. McEliece A Public-Key Cryptosystem Based On Algebraic Coding Theory // DSN Progress Report 42-44. — 1978.

[2] Jochemsz E. Goppa Codes & the McEliece Cryptosystem //Vrije Universiteit Amsterdam. – 2002. – С. 63.

[3] Bernstein D. J., Lange T., Peters C. Attacking and defending the McEliece cryptosystem //International Workshop on Post-Quantum Cryptography. – Springer, Berlin, Heidelberg, 2008. – С. 31-46.

[4] Landais G., Tillich J. P. An efficient attack of a McEliece cryptosystem variant based on convolutional codes //International Workshop on Post-Quantum Cryptography. – Springer, Berlin, Heidelberg, 2013. – С. 102-117.

[5] Baldi M. LDPC Codes in the McEliece Cryptosystem: Attacks and Countermeasures //Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. – 2009. – Т. 23. – С. 160-174.

[6] Vaidya S., Dutta S. A Study of the McEliece PKE. – 2018.

[7] Халимов Г. З., Северинов А. В. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов //Системы управления и связь.–Х.: ХВУ. – 1996. – С. 116-119.