УДК 004.056.55

Кузнецов О.О., Пушкарьов А.І., Шевцов Олексій, Кузнецова Т.Ю.
Харківський національний університет ім. В.Н. Каразіна

Несиметричне криптоперетворення з використанням алгебраїчних блокових кодів

В основі сучасних несиметричних криптоперетворень лежать такі двохключові схеми, в яких завдання пошуку секретного ключа (private key) за відомим відкритим ключем (public key) пов'язана з рішенням відомої і дуже складної математичної задачі, наприклад, факторизації, дискретного логарифмування та ін. [1-3]. У той же час у зв'язку з появою квантових обчислень, заснованих на принципах квантової механіки, швидкість вирішення деяких математичних задач значно зростає [4]. Наприклад, алгоритм Шора дозволяє знайти за кінцевий час всі прості множники великих чисел або вирішити задачу дискретного логарифмування, і, як наслідок, знайти секретний ключ в відповідних несиметричних криптосистемах, наприклад в RSA [5]. Отже, розробка нових криптографічних алгоритмів, в яких складність пошуку секретного параметра за відомим відкритим ключем залишається високою навіть з урахуванням можливого застосування квантових обчислень (тобто для пост-квантового періоду), є надзвичайно важливою науковою задачею [6, 7].

Перспективним напрямком у розвитку пост-квантової криптографії (Post-Quantum Cryptography) є кодові криптосистеми (Code-Based Cryptography). Вони засновані на використанні алгебраїчних кодів, що замасковані під код загального положення (випадковий код, повний код) [7-12]. У [7] показано, що кодові криптосистеми залишаються стійкими навіть при використанні квантових обчислень та дозволяють реалізувати відносно швидке (в порівнянні з криптосистемами RSA, ECC і ін.) криптографічне перетворення, а також реалізувати додатковий контроль помилок [8].

Першою і найбільш вивченої схемою несиметричного шифрування, заснованою на використанні алгебраїчних блокових кодів, є запропонована в 1978 році криптосистема Мак-Еліса (McEliece) [9]. Вона заснована на маскуванні лінійного алгебраїчного блокового (n,k,d) коду, який заданий над кінцевим полем $GF(q)$ породжувальною $k \times n$ матрицею G. Для маскування застосовуються невироджена $k \times k$ матриця X з елементами із $GF(q)$, діагональна $n \times n$ матриця D з ненульовими на діагоналі елементами із $GF(q)$ та переставна $n \times n$ матриця P з елементами із $GF(q)$. Криптограмою є спотворене кодове слово, тобто це вектор $c_X^* = I \cdot G_X + e$, де $c_X = I \cdot G_X$ є кодовим словом замаскованого (n,k,d) коду з породжувальною $k \times n$ матрицею $G_X = X \cdot G \cdot P \cdot D$; I – інформаційний вектор з k елементів із $GF(q)$; e – секретний випадковий вектор помилок з n елементів із $GF(q)$ з вагою Хеммінга $w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Матриці маскування X, P і D використовуються у якості секретного (приватного) ключа, а матриця G_X – у якості відкритого (публічного) ключа.

На сьогоднішній день опубліковано велику кількість різних атак на крипто-кодові схеми захисту інформації, наприклад, [11, 12], деякі виявилися досить ефективними щодо окремих варіантів кодових криптосистем. Однак базова конструкція [9] з двійковими кодами Гоппи [13, 14], що була запропонована близько 40 років тому, залишається стійкою до всіх відомих методів криптоаналізу, в тому числі і в разі використання

квантових обчислювальних систем [7]. При цьому найбільша стійкість досягається при відносній швидкості кодування $R = k / n \approx 2/3$ [8].

У таблиці 1 наведені параметри схеми Мак-Еліса з двійковими кодами Гоппи при $R \approx 2/3$, оцінки стійкості до атаки, яку засновано на алгоритмі перестановочного декодування [15, 16], оцінки обчислювальної складності криптоперетворення в порівнянні зі схемою RSA.

Таблиця 1 – Порівняльні оцінки криптосистем Мак-Еліса та RSA

Криптосистема Мак-Еліса				
Параметри двійкового *(n, k, d)* коду Гопи	Розмір ключів, біт	Складність криптоперетворення, бітових операцій	Оцінка стійкості, біт	Оцінка стійкості до квантового криптоаналізу, біт
(2048, 1300, 137)	$\approx 10^6$	$\approx 10^6$	102	49
(4096, 2584, 253)	$\approx 10^7$	$\approx 10^7$	186	91
(16384, 10322, 867)	$\approx 10^8$	$\approx 10^8$	636	310
Криптосистема RSA				
Розмір модуля, біт	Розмір ключів, біт	Складність криптоперетворення, бітових операцій	Оцінка стійкості, біт	Оцінка стійкості до квантового криптоаналізу, біт
2048	2048	$\approx 10^9$	112	40
7680	7680	$\approx 10^{11}$	192	41
15360	15360	$\approx 10^{12}$	256	44

Важлива перевага схеми Мак-Еліса полягає у високій стійкості до квантового криптоаналізу (останній стовпчик таблиці 1). У порівнянні з криптосистемою RSA складність квантового криптоаналізу схеми Мак-Еліса зі збільшенням параметрів зростає дуже швидко. Фактично при використанні квантових алгоритмів складність криптоаналізу порівнянна з рішенням переборних завдань пошуку еквівалентних ключів симетричних шифрів (оцінки стійкості в таблиці 1 наведено як раз у вигляді бітової довжини симетричного ключа).

Основним недоліком криптосистеми Мак-Еліса є величезні обсяги ключових даних (до сотень мегабіт), а також зниження відносної інформаційної швидкості, яка дорівнює $R = k / n$. Нижче показано, що цей конструктивний недолік схеми Мак-Еліса нова пропонована криптосистема частково знімає.

Іншим прикладом кодових криптосистем є схема Нідеррайтера [17], в якій також (як і в схемі Мак-Еліса) алгебраїчний код із швидким алгоритмом декодування маскується під випадковий код (декодування якого при відповідних (n,k,d) параметрах є надзвичайно складною математичною задачею). У схемі Нідеррайтера [10, 17] використовується лінійний алгебраїчний блоковий (n,k,d) код, який заданий над кінцевим полем $GF(q)$ перевірочною $(n-k)\times n$ матрицею H. Його маскують за допомогою невиродженої $k \times k$ матриці X з елементами із $GF(q)$, діагональної $n \times n$ матриці D з ненульовими на діагоналі елементами із $GF(q)$ та переставної $n \times n$ матриці P з елементами із $GF(q)$, але криптограма формується іншим чином. Інформаційні данні I спочатку перетворюються у послідовність e з n елементів із $GF(q)$ яка задовольняє умові (1), тобто вектор e розглядається як вектор помилок, який можливо виправити шляхом декодування. Криптограмою є синдромна послідовність $s_X = e \cdot H_X^T$ з $n-k$ елементів із $GF(q)$ замаскованого (n,k,d) коду з перевірочною $(n-k)\times n$ матрицею $H_X = X \cdot H \cdot P \cdot D$, причому матриці маскування X,

P і D використовується у якості секретного (приватного) ключа, а матриця H_X – у якості відкритого (публічного) ключа. В роботі [10] показано, що стійкість криптосистем Мак-Еліса і Нідеррайтера еквівалентна і ефективну атаку на одну зі схем можна легко трансформувати в атаку на іншу схему. У цьому сенсі оцінки стійкості криптосистеми Мак-Еліса, наведені в таблиці 1, справедливі і по відношенню до схеми Нідеррайтера. Інші характеристики (швидкість перетворення, обсяги ключів) також є порівняними. Щодо відносної інформаційної швидкості, вона дорівнює $R = m/(n-k)$.

Загальним конструктивним недоліком несиметричних криптосистем Мак-Еліса та Нідеррайтера є зниження відносної інформаційної швидкості. В новій пропонованій схемі цей недолік частково знімається.

За своєю суттю пропонована криптосистема є подальшим розвитком схеми Мак-Еліса з додатковим кодуванням інформаційних даних за схемою Нідеррайтера:

– в схемі Мак-Еліса інформаційні дані I розміщуються в кодовому слові $c_X = I \cdot G_X$ замаскованого коду. Зашифрування полягає в додаванні випадкового вектору помилок e, який інтерпретується як сеансовий (одноразовий) ключ. Розшифрування полягає в декодуванні вектору $c_X^* = I \cdot G_X + e$, тобто в знятті дії випадкового вектору помилок e;

– в схемі Нідеррайтера інформаційні дані I розміщуються в векторі помилок e. Далі обчислюється синдромна послідовність $s_X = e \cdot H_X^T$, яка і є криптограмою. Вектор s_X можна однозначно декодувати на приймальній стороні, тільки тепер інформаційні дані I вилучаються саме з вектору помилок e;

– в запропонованій схемі інформаційна послідовність розбивається на дві складові. Першу складову (позначимо її як вектор I_1) розмістимо в кодовому слові $c_X = I_1 \cdot G_X$; другу складову (позначимо її як вектор I_2) розмістимо в векторі помилок e. Для підвищення стійкості ці дві частини можуть бути додатково оброблені (перемішані, зашифровані і т.д.). Далі всі перетворення виконуються як в схемі Мак-Еліса, але на приймальній стороні інформація вилучається як із слова c_X (перша частина I_1), так і з вектору e (друга частина I_2). Таким чином, пропонована схема об'єднує способи перетворення інформаційних даних схем Мак-Еліса і Нідеррайтера, що дозволяє істотно підвищити відносну швидкість передачі даних, яка дорівнює $R = (k+m)/n$.

Для порівняння відносної інформаційної швидкості в таблиці 2 наведено відповідні оцінки для схем Мак-Еліса, Нідеррайтера та пропонованого способу. При розрахунках застосовувалися формули (2), (3) та (4) при $w_h(e) = t$. У якості вихідних параметрів обрано двійкові коди Гоппи із таблиці 1.

Таблиця 1 – Оцінки відносної інформаційної швидкості

	Конструктивні кодові (n,k,d) параметри		
	(2048, 1300, 137)	(4096, 2584, 253)	(16384, 10322, 867)
Схема Мак-Еліса	$R \approx 0{,}63$	$R \approx 0{,}63$	$R \approx 0{,}63$
Схема Нідеррайтера	$R \approx 0{,}57$	$R \approx 0{,}53$	$R \approx 0{,}48$
Пропонована криптосистема	$R \approx 0{,}84$	$R \approx 0{,}83$	$R \approx 0{,}81$

Очевидно, що використання запропонованої криптосистеми збільшує відносну швидкість передачі даних на 30-40% в порівнянні з кращим показником серед схем Мак-Еліса і Нідеррайтера. При цьому зберігаються всі переваги кодових криптосистем (див. таблицю 1): висока швидкість криптоперетворення (на 3-4 порядки вища ніж у схемі RSA); висока стійкість до традиційних та квантових методів криптоаналізу. Фактично слід визнати, що кодові криптосистеми є реальною альтернативою сучасних несиметричних криптосистем (RSA, ECC, або інших) в частині побудови надійних пост-квантових алгоритмів. Наведені в роботі розрахунки наочно підтверджують цей висновок. Крім того, особливості побудови кодових схем захисту інформації дозволяють одночасно з криптоперетворенням реалізувати додаткову послугу контролю помилок [8], що, безумовно, представляє інтерес для їх застосування в телекомунікаційних системах спеціального призначення.

Список використаних джерел

1. *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.*
2. *Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Вид-во «Форт», 2013. – 880с.*
3. *Arto Salomaa. Public-Key Cryptography, Second, Enlarged Edition. – Springer-Verlag, Berlin, Heidelberg, New York, 1996. – x+271 pp.*
4. *Nigel Smart. Cryptography: An Introduction (3rd Edition). – 432 pp. https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf*
5. *Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Foundations of Computer Science : Conference Publications. – 1994. – P. 124-134.*
6. *Neal Koblitz and Alfred J. Menezes. A Riddle Wrapped in an Enigma. https://eprint.iacr.org/2015/1018.pdf*
7. *Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p.*
8. *Кузнецов А.А. Алгебраическая теория блоковых кодов и ее приложения в криптографии // Перша міжнародні наукова конференція 25–27 травня 2005р. „Теорія та методи обробки сигналів”. Тези доповідей. – К.: НАУ. – 2005. – С. 6 – 8.*
9. *McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978. P. 114-116.*
10. *Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.*
11. *Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона. // Дискретная математика. – 1992. – Т.4.№3. – С.57-63.*
12. *Daniel J. Bernstein and Tanja Lange and Christiane Peters. Attacking and defending the McEliece cryptosystem. https://cr.yp.to/codes/mceliece-20080807.pdf*
13. *В. Д. Гопла. Новый класс линейных корректирующих кодов // Пробл. передачи информ., 1970, том 6, выпуск 3, С. 24–30.*
14. *В. Д. Гопла. На неприводимых кодах достигается пропускная способность ДСК. // Пробл. передачи информ., 1974, том 10, выпуск 1, С. 111–112.*
15. *Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications. – Springer, 1981, - 432 p.*
16. *F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes. – North-Holland, Amsterdam, New York, Oxford, 1977, – 762 pp.*
17. *Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. P. 19-34.*
18. *Метод недвійкового рівновагового кодування / В. Б. Дудикевич, О. О. Кузнєцов, Б. П. Томашевський // Сучасний захист інформації. - 2010. - № 3. - С. 57-68.*
19. *Дудикевич В.Б., Кузнецов О.О., Томашевський Б.П., Максимович В.М. Спосіб формування рівновагових недвійкових послідовностей. Пат. UA 94308 U, МКІ (2006.01) H03M 7/06. – № и 2009 08173; Заявл. 03.08. 2009; Опубл. 24.04.2011, Бюл. №8, 2011р. – 4с.*