УДК 004.056.55:519.725

О. О. Кузнецов*,,** д-р. техн. наук, професор,
А. І. Пушкарьов*,**
Ю. І. Горбенко,** канд. техн. наук

* Харківський національний університет імені В. Н. Каразіна, м. Харків,
** ПАТ «Інститут інформаційних технологій», м. Харків,
*** Державна служба спеціального зв'язку
та захисту інформації України, м. Київ

КОДОВІ КРИПТОСИСТЕМИ ДЛЯ ПОСТКВАНТОВОГО ЗАСТОСУВАННЯ

Розглядаються кодові криптосистеми з відкритим ключем. В їх основі лежить маскування алгебраїчних блокових кодів з швидким (поліноміальної складності) алгоритмом декодування під випадковий лінійний блоковий код з NP-складним декодуванням. Наводяться оцінки стійкості, в тому числі, до квантового криптоаналізу, а також оцінки швидкодії в порівнянні з відомими криптосистемами.

Ключові слова: *кодова криптосистема, пост-квантовий період, алгебраїчне кодування.*

Вступ. Останнім часом несиметричні криптоперетворення набули широкого розповсюдження. Однак з появою квантових обчислень, заснованих на принципах квантової механіки, швидкість вирішення деяких математичних задач значно зростає [1–3]. Наприклад, алгоритм Шора дозволяє знайти за кінцевий час всі прості множники великих чисел або вирішити задачу дискретного логарифмування, і, як наслідок, знайти секретний ключ у відповідних несиметричних криптосистемах, наприклад, в RSA, ECC, тощо [3]. Отже, розробка нових криптографічних алгоритмів, в яких складність пошуку секретного параметра за відомим відкритим ключем залишається високою з урахуванням застосування квантових обчислень (для пост-квантового періоду), є надзвичайно важливою науковою задачею.

Перспективним напрямком у розвитку пост-квантової криптографії (Post-Quantum Cryptography) є кодові криптосистеми (Code-Based Cryptography) [4–6]. Вони засновані на використанні алгебраїчних кодів, що замасковані під код загального положення (випадковий код, повний код), та залишаються стійкими навіть при використанні квантових обчислень.

Метою роботи є дослідження стійкості кодових криптосистем, в тому числі до квантового криптоаналізу, а також оцінка швидкодії в порівнянні з відомими криптосистемами.

Виклад основного матеріалу. Першою і найбільш вивченою кодовою криптосистемою є запропонована в 1978 році схема Мак-Еліса (McEliece) [4]. Вона заснована на маскуванні лінійного алгебраїчного блокового (n,k,d) коду, який задано 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 Хемінга $w_h(e) \le t = \lfloor (d-1)/2 \rfloor$. Матриці маскування X, P і D використовуються у якості секретного (приватного) ключа, а матриця G_X — у якості відкритого (публічного) ключа.

Зловмиснику необхідно декодувати криптограму c_X^* використовуючи відому йому породжувальну матрицю G_X. Однак декодування випадкового коду (при відповідних параметрах (n,k,d) і $w_h(e)$) є обчислювально недосяжним. Не знаючи матриці X, P і D, зловмисник не може відновити матрицю G і скористатися алгоритмом декодування поліноміальної складності. З цих міркувань величину $w_h(e)$ слід максимізувати. Наприклад, при $w_h(e) = t$ складність декодування буде максимальною, що забезпечить найвищий рівень стійкості кодової криптосистеми для заданих параметрів (n,k,d).

Іншим прикладом кодових криптосистем є схема Нідеррайтера [5], в якій також (як і в схемі Мак-Еліса) алгебраїчний код зі швидким алгоритмом декодування маскується під випадковий код (декодування якого при відповідних (n,k,d) параметрах є надзвичайно складною математичною задачею).

У схемі Нідеррайтера [5, 6] 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 дані 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 використовуються як секретний (приватний) ключ, а матриця H_X — як відкритий (публічний) ключ.

Найбільш природнім напрямком у розвитку методів криптоаналізу кодових схем є використання неалгебраїчних методів декодування. Серед універсальних методів декодування лінійних блокових кодів, заданих довільною породжуючою матрицею, особливе місце займають перестановочні алгоритми [7, 8]. Основна ідея такого декодування полягає у використанні різних наборів покрівельних множин. Найменша кількість множин, які можуть виправити всі комбінації з t помилок, обмежується виразом [7]:

$$N \geq \frac{n!(n-k-t)!}{(n-t)!(n-k)!}.$$

На рисунку показані залежності найменшого числа покрівельних множин, які потрібні для виправлення всіх комбінації з t помилок довільного лінійного блокового коду. Оцінки N наведено в логарифмічному масштабі в залежності від відносної швидкості кодування $R = k/n$ і розраховані для параметрів двійкових сепарабельних кодів Гоппи [9, 10]:

$$n = 2^m,\ k \geq n - mr,\ r = \deg G(x),\ d \geq 2r + 1,$$

де $deg\ G(x)$ — степінь многочлена Гоппи $G(x)$, $m \in N$. Наведені на рисунку залежності слід інтерпретувати як оцінки стійкості кодових криптосистем, що виражено в кількості покриваючих множин, котрі потрібно перебрати для декодування будь-якої конфігурації вектора помилок. При цьому найбільша стійкість забезпечується при використанні кодів з відносною швидкістю $R \approx 2/3$, що узгоджується з висновками більшості досліджень [1, 11].

У таблиці наведено параметри деяких схем з кодами Гоппи і $R \approx 2/3$, оцінки стійкості до атаки перестановочного декодування, оцінки обчислювальної складності кодування (шифрування) і декодування (розшифрування), а також аналогічні оцінки для несиметричних криптосистем RSA і ECC. Наведені значення наочно розкривають переваги і недоліки кодових криптосистем. Декодування випадкового коду — надзвичайно складна обчислювальна задача і переборний пошук, ймовірно, є найкращим з відомих на сьогоднішній день

її рішенням. Квантові обчислення прискорюють цей процес, що знижує тимчасові витрати криптоаналізу, але це зниження не є критичним (приблизно в два рази зменшується еквівалентна довжина ключа). Фактично слід визнати, що кодові криптосистеми є реальною альтернативою сучасних асиметричних криптосистем (RSA, ECC, або інших) в частині побудови надійних постквантових алгоритмів. Наведені в роботі розрахунки наочно підтверджують цей висновок.

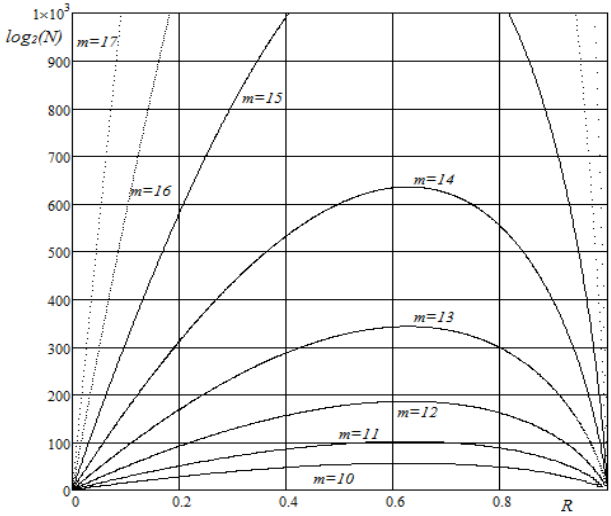

Рисунок. *Оцінка стійкості схеми Мак-Еліса на сепарабельних двійкових кодах Гоппи до атаки декодуванням перестановкою*

Таблиця

Ефективність кодових криптосистем в порівнянні з RSA и ECC

	Розмір ключів, біт	**Складність реалізації, бітових операцій**	**Стійкість, біт**	**Стійкість до квантового криптоаналізу, біт**
Достатній рівень стійкості (100..128 біт)				
Кодова криптосистема, двійковий код Гоппи (2048, 1300, 137)	1,6 .. 2,6 Мбіт	10^6 .. 10^7	102	49
Криптосистема RSA, порядок модуля 2^{2048}	2048 біт	10^{10}	112	35
Криптосистема RSA, порядок модуля 2^{3072}	3072 біт	10^{11}	128	37
Криптосистема ECC, порядок поля 2^{224}	448 біт	10^9	112	32

Продовження таблиці

Криптосистема ECC, порядок поля 2^{256}	512 біт	10^{10}	128	32
Високий рівень стійкості (180..256 біт)				
Кодова криптосистема, двійковий код Гоппи (4096, 2584, 253)	6 .. 10 Мбіт	10^{7}	186	91
Криптосистема RSA, порядок модуля 2^{7680}	7680 біт	10^{12}	192	41
Криптосистема RSA, порядок модуля 2^{15360}	15360 біт	10^{13}	256	44
Криптосистема ECC, порядок поля 2^{384}	768 біт	10^{11}	192	34
Криптосистема ECC, порядок поля 2^{512}	1024 біт	10^{12}	256	35
Надвисокий рівень стійкості (> 256 біт)				
Кодова криптосистема, двійковий код Гоппи (8192, 5163, 467)	27 .. 42 Мбіт	10^{8}	343	167
Кодова криптосистема, двійковий код Гоппи (16384, 10322, 867)	106 .. 170 Мбіт	10^{8} .. 10^{9}	636	310
Криптосистема ECC, порядок поля 2^{768}	1536 біт	10^{13}	384	37
Криптосистема ECC, порядок поля 2^{1024}	2048 біт	10^{14}	512	38

Основним недоліком кодових схем є величезні ключові дані. Для розглянутих прикладів обсяги ключів досягають сотень мегабіт і поки не представляється можливим їх зменшити без зниження стійкості криптосистеми. Ключі в кодових схемах — це генераторні (породжують і / або перевірочні) матриці лінійного коду, які повинні виглядати для зловмисника як випадковий набір лінійно незалежних векторів. Стиснути або якимось чином зменшити цей набір не представляється можливим.

Висновки. Несиметричні криптосистеми на основі алгебраїчних блокових кодів було запропоновано близько 40 років тому і сприймалися тоді більшістю дослідників як екзотичний і малопрактичний напрямок у криптографії. Очевидні недоліки (великі обсяги ключових даних і зниження відносної швидкості передачі) протягом тривалого часу стримували їх подальший розвиток і практичне використання. І тільки за останні роки, коли стало зрозуміло, що багато існуючих, стандартизованих і широко використовуваних на практиці криптоалгоритмів можуть виявитися беззахисними проти атак квантового криптоаналізу, кодові криптосистеми отримали заслужену увагу дослідників.

Декодування випадкового коду — надзвичайно складна обчислювальна задача і переборний пошук при її вирішенні, ймовірно, є

найкращим з відомих на сьогоднішній день варіантів. Квантові алгоритми прискорюють цей процес, що знижує часові витрати криптоаналізу, але це зниження не є критичним (приблизно в два рази зменшується еквівалентна довжина ключа). Фактично слід визнати, що кодові криптосистеми є реальною альтернативою сучасним несиметричним криптосистемам (RSA, ECC та інших) в частині побудови надійних пост-квантових алгоритмів. Наведені в роботі розрахунки наочно підтверджують цей висновок. Крім того, особливості побудови кодових схем дозволяють одночасно з криптозахистом реалізувати додаткову послугу контролю помилок, які виникають при передачі інформації за реальними каналами передачі сигналів з перешкодами. Ця особливість, безумовно, представляє інтерес для їх застосування в телекомунікаційних системах спеціального призначення.

Список використаних джерел:

1. Bernstein D., Buchmann J., Dahmen E. Post-quantum cryptography. Berlin: Springer, 2009. 246 p.
2. Post-quantum cryptography project. National Institute of Standards and Technology. http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html.
3. John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv.quant-ph/0301141 v2, 2004.
4. 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.
5. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. Problem Control and Inform Theory, 1986. Vol. 15. P. 19–34.
6. Сидельников В. М. Криптография и теория кодирования. Материалы конференции *«Московский университет и развитие криптографии в России»*, МГУ. 2002. 22 с.
7. Clark G. C., Cain J. B. Error-Correction Coding for Digital Communications. Springer, 1981. 432 p.
8. MacWilliams F. J., Sloane N. J. A. The theory of error-correcting codes. North-Holland, Amsterdam, New York, Oxford, 1977. 762 p.
9. Гоппа В. Д. Новый класс линейных корректирующих кодов. Проблемы передачи информации, 1970. Том 6, Вып. 3. С. 24–30.
10. Гоппа В. Д. На неприводимых кодах достигается пропускная способность ДСК. Проблемы передачи информации. 1974. Том 10. Вып. 1. С. 111–112.
11. Raphael Overbeck, Nicolas Sendrier, Code-based cryptography. In: Daniel J. Bernstein, et al. (eds). First International Workshop on Post-quantum Cryptography, PQ Crypto 2006, Leuven, The Netherland, May 23–26, 2006. Selected papers, P. 95–145.

Code-based public-key cryptosystems based on algebraic coding are considered. They are based on masking algebraic block codes with fast decoding algorithm (polynomial complexity) at random linear block code with NP-hard

decoding. Assessment the strength is offered, including quantum cryptanalysis, and evaluating performance in comparison with the known cryptosystems.

Key words: *code-based cryptosystems, post-quantum period, algebraic coding.*

Одержано 23.03.2017

УДК 681.3.06

К. Є. Лисицький, аспірант

Харківський національний університет імені В. Н. Каразіна, м. Харків

ОПТИМІЗАЦІЯ ПЕРСПЕКТИВНИХ АЛГОРИТМІВ СИМЕТРИЧНОГО БЛОЧНОГО ПЕРЕТВОРЕННЯ ПО КРИТЕРІЯМ ШВИДКОДІЇ І СТІЙКОСТІ

Розглядаються принципи побудови шифру Rijndael, застосовані розробниками, що дозволили цього шифру зайняти лідируючі позиції в технологіях проектування та розробки блокових симетричних шифрів. Як друга прогресивна розробка відзначається шифр IDEA NXT. Наводяться результати аналізу перспективності рішень, прийнятих у цих розробках. Відзначається, що, незважаючи на їх новизну і досягнуті високі показники ефективності розглянутих рішень, дослідження, проведені останнім часом, свідчать про можливості їх подальшого поліпшення, про можливості побудови більш досконалої конструкції шифрувального перетворення. Ці можливості враховані в запропонованій новій концепції проектування блочних симетричних шифрів, що будується на ряді висунутих положень. Її реалізація демонструється на прикладі розробки однієї з нових конструкцій шифру і його модифікації, побудованих на основі використання принципів керованих підстановлювальних перетворень. Запропоновані конструкція за простотою і прозорістю рішень, за показниками доказової стійкості до атак диференціального і лінійного криптоаналізу, а також за показниками продуктивності не поступаються визнаному лідеру технологій блочного симетричного шифрування шифру Rijndael (AES), а по динаміці приходу шифру до стану випадкової підстановки вони перевершують практично всі відомі рішення.

Ключові слова: *технології проектування і розробки блочних симетричних шифрів, матричне лінійне перетворення, ефективність шифруючого перетворення, нова концепція проектування і розробки БСШ, лінійне перетворення з керуючими підстановками, випадкові підстановки, динамічні показники приходу шифру до випадкової підстановки.*

Розглядаються конструкції двох сучасних розробок з побудови блочних симетричних шифрів: шифр Rijndael і шифр IDEA NXT. Розглядаються також свіжі розробки — шифри Мухомор, Калина-2 і бі-