DOI: 10.18372/2410-7840.18.11088
УДК 004.056.55

НЕСИМЕТРИЧНЕ КРИПТОГРАФІЧНЕ ПЕРЕТВОРЕННЯ З ВИКОРИСТАННЯМ АЛГЕБРАЇЧНИХ БЛОКОВИХ КОДІВ

Олександр Кузнецов, Андрій Пушкарьов, Олексій Шевцов, Тетяна Кузнецова

Можливість появи квантового комп'ютера ставить під загрозу існування багатьох асиметричних криптопримітивів. Важливою перевагою кодових криптосистем є висока стійкість до квантового криптоаналізу. Разом із цим сучасний розвиток інформаційних технологій створює потребу вдосконалювати швидкодію систем на кодах та їх захищеність від класичного криптоаналізу. Розглянуто несиметричні криптосистеми на алгебраїчних кодах, досліджено сучасний стан, існуючі протиріччя і перспективи їх практичного застосування на постквантовий період. Отримано оцінки стійкості до атаки, яку засновано на алгоритмі перестановочного декодування, оцінки обчислювальної складності криптоперетворення в порівнянні зі схемою RSA. Запропоновано нову кодову криптосистему, в якій вдається суттєво підвищити відносну інформаційну швидкість зі збереженням основних переваг щодо стійкості до класичного та квантового криптоаналізу.

Ключові слова: *криптосистеми на алгебраїчних кодах, постквантова криптографія.*

Вступ. В основі сучасних несиметричних криптоперетворень лежать такі двоключові 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 у 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 постквантової 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].

Метою даної роботи є дослідження сучасного стану несиметричних криптосистем на алгебраїчних кодах, існуючих протиріч і перспектив практичного застосування на постквантовий період.

1. Криптосистема Мак-Еліса. Першою і найбільш вивченої схемою несиметричного шифрування, заснованою на використанні алгебраїчних блокових кодів, є запропонована в 1978 році криптосистема Мак-Еліса (McEliece) [9].

Схема Мак-Еліса [9, 10] 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

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor. \quad (1)$$

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

Вектор e слід розглядати як одноразовий сеансовий секретний ключ, його вага визначає складність декодування спотвореного кодового слова (криптограми).

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).

Для уповноваженого користувача (який знає секретний ключ) декодування є задача з поліноміальною складністю вирішення. Дійсно, легітимний користувач, отримавши вектор c_X^*, будує вектор

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}.$$

Матриця $\Lambda = D^{-1} \cdot P^{-1}$ зберігає вагу і відстань по Хеммінгу, тобто для будь-яких кодових слів c і c' виконуються рівності:

$$w_h(c) = w_h(c \cdot \Lambda),$$

$$w_h(c,c') = w_h(c \cdot \Lambda, c' \cdot \Lambda).$$

Це означає, що вектор $\bar{c}^*$ є спотвореним не більше, ніж в $w_h(e)$ розрядах кодовим словом алгебраїчного коду з породжувальною матрицею G і його можна декодувати швидким алгоритмом поліноміальної складності. Таким чином, уповноважений користувач декодує вектор

$$\bar{c}^* = I' \cdot G + e',$$

тобто знаходить I', після чого обчислює інформаційний вектор $I = I' X^{-1}$.

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 Гопи [13, 14], запропонована близько 40 років тому, залишається стійкою до всіх відомих методів криптоаналізу, в тому числі, в разі використання квантових обчислювальних систем [7]. При цьому найбільша стійкість досягається при відносній швидкості кодування $R = \frac{k}{n} \approx \frac{2}{3}$ [8].

У таблиці 1 наведено параметри схеми Мак-Еліса з двійковими кодами Гопи 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. 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 порівняна з рішенням переборних завдань пошуку еквівалентних ключів симетричних шифрів (оцінки стійкості в таблиці 1 наведено як раз у вигляді бітової довжини симетричного ключа).

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

Основним недоліком криптосистеми Мак-Еліса є величезні обсяги ключових даних (до сотень мегабіт), а також зниження відносної інформаційної швидкості, яка дорівнює

$$R = \frac{k}{n}. \quad (2)$$

Нижче показано, що цей конструктивний недолік схеми Мак-Еліса частково знімається новою пропонованою криптосистемою, тобто вдається суттєво підвищити відносну інформаційну швидкість.

2. Криптосистема Нідеррайтера. Іншим прикладом кодових криптосистем є схема Нідеррайтера [17], 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 [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 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. Відповідний інформаційний вектор I, який буде містити тільки

$$m = \left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor$$

елементів із $GF(q)$, перетворюється на вектор e із застосуванням методів рівновагового кодування, які викладено, наприклад в [18, 19]. Для найбільшої стійкості криптоперетворення треба застосовувати вектор e з $w_h(e)=t$ і тоді

$$m = \left\lfloor \log_q \left((q-1)^t \frac{n!}{t!(n-t)!} \right) \right\rfloor.$$

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.

Для розшифрування криптограми s_X уповноважений користувач знімає дію матриць маскування, декодує отримане слово і знаходить вектор помилок e, за яким відновлює інформаційний вектор I. 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 розумінні 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, в криптосистемі Нідеррайтера вона дорівнює

$$R = \frac{m}{n-k}. \quad (3)$$

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

3. Пропонована криптосистема. За своєю суттю пропонована криптосистема є подальшим розвитком схеми Мак-Еліса з додатковим кодуванням інформаційних даних за схемою Нідеррайтера. На рис. 1 схематично зображено процес криптографічного перетворення з використанням кодів:

– 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).

Пропоноване несиметричне криптоперетворення з використанням алгебраїчних блокових кодів ґрунтується на тому, що лінійний блоковий (n,k,d) код, який заданий над кінцевим полем $GF(q)$ породжувальною $k \times n$ матрицею G, маскується невиродженою $k \times k$ матрицею X з елементами із $GF(q)$, діагональною $n \times n$ матрицею D з ненульовими на діагоналі елементами із $GF(q)$, переставною $n \times n$ матрицею P з елементами із $GF(q)$ а інформаційні данні розміщуються у двох складових (векторах I_1 та I_2).

Криптограма формується за правилом

$$c_X^* = I_1 \cdot G_X + e,$$

де вектор $c_X = I_1 \cdot G_X$ є кодовим словом замаскованого (n,k,d) коду з породжувальною $k \times n$ матрицею

$$G_X = X \cdot G \cdot P \cdot D.$$

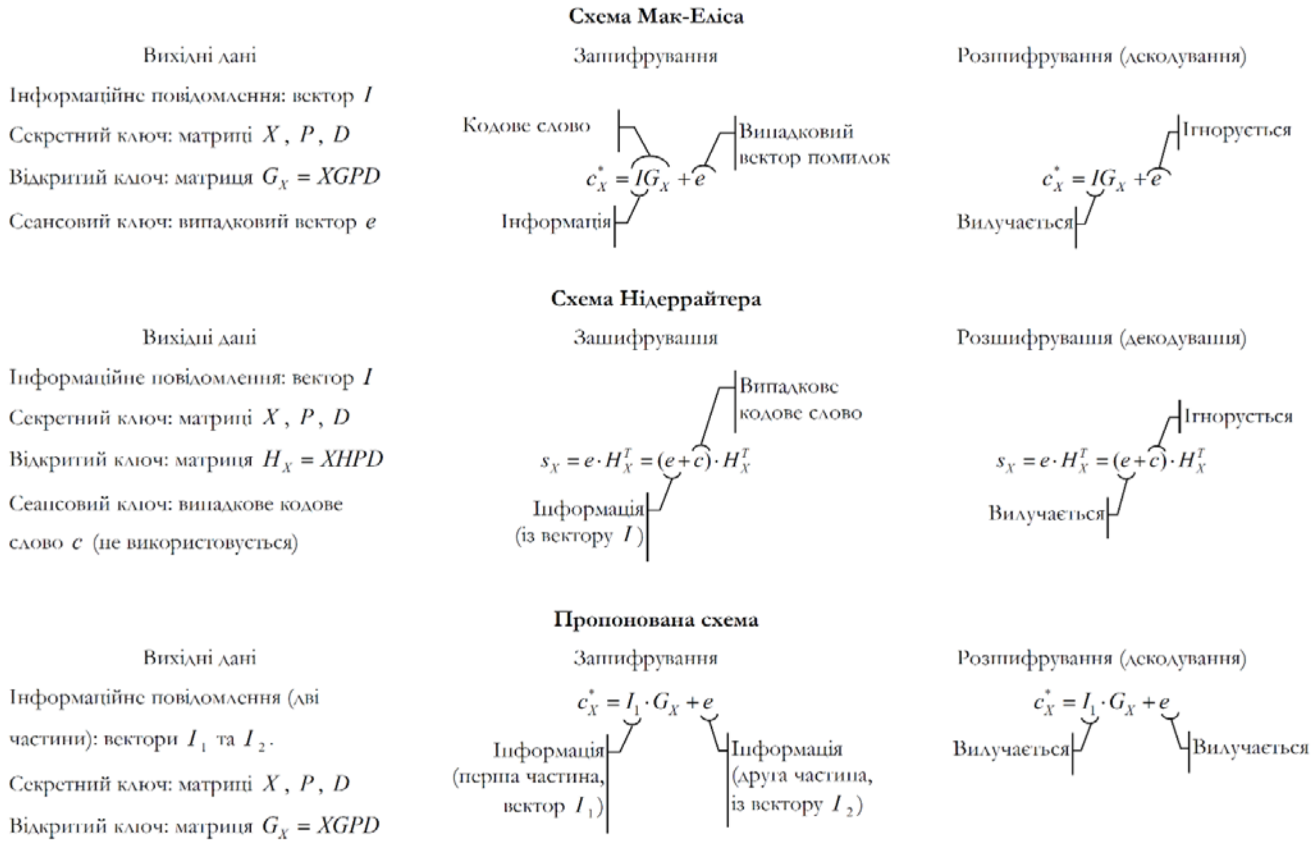

Рис. 1. Криптографічне перетворення у відомих кодових схемах (Мак-Еліса та Нідеррайтера) та в пропонованій криптосистемі.

Таким чином, кодове слово c_X формується за першою складовою інформаційних даних I_1, тобто як і в схемі Мак-Еліса – за вектором з k елементів із $GF(q)$.

Друга складова інформаційних даних I_2 обробляється як у схемі Нідеррайтера, а саме вектор I_2 з m елементів із $GF(q)$ перетворюється у вектор e – закодований інформаційний вектор (аналог вектору помилок) з n елементів із $GF(q)$, для якого виконуються обмеження:

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

$$m = \left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor.$$

Для найбільшої стійкості криптоперетворення треба застосовувати вектор e, що задовольняє обмеженням:

$$w_h(e) = t\,,\ m = \left\lfloor \log_q \left((q-1)^t \frac{n!}{t!(n-t)!} \right) \right\rfloor.$$

Для перетворення вектору I_2 з m елементів із $GF(q)$ у вектор e з n елементів із $GF(q)$ та $w_h(e) = t$ треба застосовувати різні способи рівновагового кодування, які викладено, наприклад в [18, 19].

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

Таким чином, інформаційні данні у пропонованій криптосистемі розміщуються у двох складових криптограми c_X^*, а саме:

– у кодовому слові c_X, що сформоване за вектором I_1 (як у схемі Мак-Еліса),

– у векторі помилок e, що сформований за другою складовою I_2 (як у схемі Нідеррайтера).

Тобто пропонована схема об'єднує способи перетворення інформаційних даних схем Мак-Еліса і Нідеррайтера, що дозволяє істотно підвищити відносну швидкість передачі даних, яка дорівнює

$$R = \frac{k+m}{n}. \tag{4}$$

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 Гопи із таблиці 1.

Таблиця 2

Оцінки відносної інформаційної швидкості

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

Висновки. 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 постквантових 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.

ЛІТЕРАТУРА

[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. – 880 с.

[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 p. 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. – pp. 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. pp. 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. Гоппа. Новый класс линейных корректирующих кодов // Пробл. передачи информ., 1970, том 6, выпуск 3, С. 24–30.
[14]. В.Д. Гоппа. 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 p.
[17]. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. pp. 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, MKI (2006.01) H03M 7/06. – № u 2009 08173; Заявл. 03.08. 2009; Опубл. 24.04.2011, Бюл. №8, 2011р. – 4 с.

REFERENCES

[1]. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.
[2]. Gorbenko I.D., Gorbenko Yu.I. Prikladna kriptologiya. Teoriya. Praktika. Zastosuvannya: Pidruchnik dlya vishchikh navchal'nikh zakladiv. – Kharkiv: Vid-vo «Fort», 2013. – 880 p.
[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 p. 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. – pp. 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]. Kuznetsov A.A. Algebraicheskaya teoriya blokovykh kodov i ee prilozheniya v kriptografii // Persha mizhnarodni naukova konferentsiya 25–27 travnya 2005r. „Teoriya ta metodi obrobki signaliv”. Tezi dopovidei. – K.: NAU. – 2005. – pp. 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. pp. 114-116.
[10]. Sidel'nikov V.M. Kriptografiya i teoriya kodirovaniya. Materialy konferentsii «Moskovskii universitet i razvitie kriptografii v Rossii», MGU. – 2002. – 22 p.
[11]. Sidel'nikov V.M., Shestakov S.O. O sisteme shifrovaniya, postroennoi na osnove obobshchennykh kodov Rida-Solomona. // Diskretnaya matematika. – 1992. – T.4.№3. – pp. 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]. V. D. Goppa. Novyi klass lineinykh korrektiruyushchikh kodov // Probl. peredachi inform., 1970, tom 6, vypusk 3, pp. 24–30.
[14]. V. D. Goppa. Na neprivodimykh kodakh dostigaetsya propusknaya sposobnost' DSK. // Probl. peredachi inform., 1974, tom 10, vypusk 1, pp. 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 p.
[17]. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. pp. 19-34.
[18]. Metod nedvijkovogo rivnovagovogo koduvannja / V.B. Dudykevych, O.O. Kuznjecov, B.P. Tomashevs'kyj // Suchasnyj zahyst informacii'. - 2010. - № 3. - pp. 57-68.
[19]. Dudykevych V.B., Kuznecov O.O., Tomashevs'kyj B.P., Maksymovych V.M. Sposib formuvannja rivnovagovyh nedvijkovyh poslidovnostej. Pat. UA 94308 U, MKI (2006.01) H03M 7/06. – № u 2009 08173; Zajavl. 03.08. 2009; Opubl. 24.04.2011, Bjul. №8, 2011r. – p. 4 .

НЕСИММЕТРИЧНОЕ КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ С ИСПОЛЬЗОВАНИЕМ АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДОВ

Возможность появления квантового компьютера ставит под угрозу существование многих асимметричных криптопримитивов. Важным преимуществом кодовых криптосистем является высокая устойчивость к квантовому криптоанализу. Вместе с этим современное развитие информационных технологий создает необходимость совершенствовать быстродействие систем на кодах и их защищенность от классического криптоанализа. Рассмотрены несимметричные криптосистемы на алгебраических кодах, исследованы современное состояние, существующие противоречия и перспективы их практического применения на постквантовый период. Получены оценки стойкости к атаке, основанной на алгоритме перестановочного декодирования, оценки вычислительной сложности криптопреобразования по сравнению со схемой RSA. Предложена новая кодовая криптосистема, в которой удается существенно повысить относительную информационную скорость с сохранением основных преимуществ по стойкости к классическому и квантовому криптоанализу.

Ключевые слова: криптосистемы на алгебраических кодах, постквантовая криптография.

PUBLIC-KEY CODE-BASED CRYPTOGRAPHY

The possibility of a quantum computer threatens the existence of many asymmetric cryptographic primitives. An important advantage of code cryptosystems is the high resistance to the quantum cryptanalysis. Therefore it is in great demand increasing the speed of the code based primitives and their protection from classical cryptanalysis. Code-Based Public-Key Cryptosystems based on algebraic coding are considered in this paper. In addition, the current state, the existing contradictions and prospects of practical use for the post-quantum period are studied. We consider estimation of resistance to attack permutation decoding and computational complexity compared to the RSA scheme. We proposed a new code cryptosystem, it significantly increases the relative information performance and keeps the main advantages of resistance to classical and quantum cryptanalysis.

Keywords: Code-Based Cryptosystems, post-quantum cryptography

Кузнецов Олександр Олександрович, доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: kuznetsov@karazin.ua

Кузнецов Александр Александрович, доктор технических наук, профессор, профессор кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г.. Харьков, Украина.

Kuznetsov Olexandr, Doctor of science (habilitation)**,** Professor of Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Пушкарьов Андрій Іванович, директор департаменту Державної служби спеціального зв'язку та захисту інформації України, м. Київ, Україна.
E-mail: s1necerra@gmail.com.

Пушкарев Андрей Иванович, директор департамента Государственной службы специальной связи и защиты информации Украины, г. Киев, Украина.

Pushkarev Andriy, Director of the State Service of Special Communication and Information Protecion of Ukraine, Kyiv, Ukraine.

Шевцов Олексій Володимирович, молодший науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: s1necerra@gmail.com

Шевцов Алексей Владимирович, младший научный сотрудник кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г. Харьков, Украина.

Shevtsov Oleksiy, junior research fellow**,** Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Кузнецова Тетяна Юріївна, науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна, м. Харків, Україна.
E-mail: s1necerra@gmail.com

Кузнецова Татьяна Юрьевна, научный сотрудник кафедры безопасности информационных систем и технологий Харьковского национального университета им. В.Н. Каразина, г. Харьков, Украина.

Kuznetsova Tetjna, research fellow, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.