УДК 004.056.5

О.О. КУЗНЕЦОВ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
А.С. КІЯН, А.О. УВАРОВА, Т.Ю. КУЗНЕЦОВА

ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ГІБРИДНОЇ КОДОВОЇ КРИПТОСИСТЕМИ

1. Вступ

Переважна більшість сучасних криптографічних систем побудована на механізмах, які забезпечують захист завдяки складності вирішення певної математичної задачі такої, як дискретне логарифмування, факторизація тощо [1, 2]. На противагу, криптосистеми, що засновані на кодуванні, нині не застосовуються широким загалом, але у найближчий час все може докорінно змінитися. Ця зміна обумовлена прагненням світової спільності створити повномасштабний квантовий комп'ютер, який буде здатен прискорити виконання операцій звичайного комп'ютера в десятки чи навіть сотні разів [3]. З огляду на це актуальними стали дослідження у лоні постквантової криптографії, тобто криптографії, що представляє алгоритми, які є стійкими до квантового та класичного криптоаналізу. Існує чотири основних напрямків досліджень: криптографія, заснована на геш-функціях; криптографія, заснована на алгебраїчних решітках; криптографія, заснована на факторизації поліномів та криптографія, заснована на завадостійких кодах [4]. У дослідженні ми зосереджуємо увагу саме на останньому напрямку, зважаючи на декілька факторів. По-перше, системи, засновані на кодах, здатні надавати такі переваги, як контроль помилок у каналі. По-друге, висока швидкість криптоперетворення та доведена стійкість до класичного і квантового криптоаналізу відрізняють кодові системи від їх конкурентів [5]. Найпопулярнішими криптосистемами, що базуються на використанні кодування, є схеми Мак-Еліса та Нідеррайтера.

Проаналізувавши їх структуру, переваги та недоліки, ми пропонуємо нову, так звану, гібридну криптосистему, що поєднує принципи зашифрування двох вищезгаданих систем та надає додаткові суттєві переваги, що будуть розглянуті надалі.

2. Дослідження принципів побудови кодових схем

2.1. Криптосистема Мак-Еліса

Криптосистема Мак-Еліса є так званою класичною криптосистемою, що базується на використанні кодів. Вона була запропонована більше 30 років тому і досі вважається стійкою не тільки до класичного, а й до квантового криптоаналізу. Сутність даної схеми можна визначити як маскування швидкого правила декодування за допомогою матричного множення породжуючої матриці алгебраїчного блокового коду на випадкові матриці (що є секретними ключами) [6]. Зловмисник, тобто той, хто має тільки відкритий ключ, повинен використати складний алгоритм неалгебраїчного декодування. Цей алгоритм визначається як NP-повна задача. Уповноважений користувач, який має секретний ключ, знімає дію маскуючих матриць і застосовує швидкий алгебраїчний алгоритм декодування. Далі визначимо алгоритм шифрування за допомогою схеми Мак-Еліса:

1). Зафіксуємо скінчене поле $GF(q)$. G – породжуюча матриця (n,k,d) кода над $GF(q)$, X – невироджена $k\times k$ матриця з елементами з $GF(q)$, P та D – перестановочна та діагональна $n\times n$ матриці відповідно (для двійкових кодів матриця D не використовується).

2). Сформуємо матрицю $G_X = X\cdot G\cdot P\cdot D$. Вона є відкритим ключем схеми Мак-Еліса. При цьому матриці X, P та D є секретним ключем.

3). Криптограма формується згідно з наступним правилом:

$$c_X^* = I\cdot G_X + e, \tag{1}$$

де e – це вектор помилок, вага Хемінга якого відповідає вимозі:

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

I – k-розрядний інформаційний вектор над полем $GF(q)$.

Виконавши згадані кроки, отримаємо кодове слово $c_X = I \cdot G_X$, що викривлене вектором помилок. У цьому випадку вектор e слід розглядати як одноразовий секретний ключ. Його вага визначає складність декодування спотвореного кодового слова (криптограми) [7].

Алгоритм розшифрування можна описати такими кроками:

1) Побудування вектору $\overline{c}^{*} = c_X^{*} \cdot D^{-1} \cdot P^{-1}$. Матриця $\Lambda = D^{-1} \cdot P^{-1}$ зберігає відстань і вагу за Хемінгом. Це означає, що побудований вектор є спотвореним не більше, ніж у $w_h(e)$ розрядів. Для двійкових кодів цей крок трохи відрізняється, оскільки у такому випадку ми не використовуємо матрицю D і побудова вектора зводиться до множення $\overline{c}^{*} = c_X^{*} \cdot P^{-1}$.

2) При використанні алгоритму поліноміальної складності декодування вектору $\overline{c}^{*} = I' \cdot G + e'$, тобто знаходження I'.

3) Обчислення початкового k-розрядного інформаційного вектора $I = I' X^{-1}$ [6-7].

Отже, розшифрування за схемою Мак-Еліса виконується завдяки зняттю дії маскуючих матриць та використанню алгоритму декодування, що має поліноміальну складність [8].

2.2. Криптосистема Нідеррайтера

Наступним кроком розглянемо особливості функціонування теоретико-кодової схеми Нідеррайтера (Niederreiter). Вона заснована також на перевагах використання маскуючих матриць, як у схемі Мак-Еліса [7 – 9]. Визначимо алгоритм шифрування, що виконується у даній схемі:

1) Зафіксування скінченого поля $GF(q)$. Нехай H – перевірочна матриця алгебраїчного (n,k,d) коду над $GF(q)$ (в оригінальній статті було запропоновано використовувати узагальнені коди Ріда – Соломона).

2) Формування секретного ключа, що містить такі складові: X – невироджена $(n-k)\times(n-k)$ матриця з елементами з $GF(q)$, P – перестановочна $n \times n$ матриця, D – діагональна $n \times n$ матриця (для двійкових кодів ця матриця не використовується).

3) Обчислення відкритиого ключа схеми згідно з правилом

$$H_X = X \cdot H \cdot P \cdot D.$$

4) Формування криптограми здійснюється за рахунок множення вектора e на транспонований відкритий ключ:

$$s_X = e \cdot H_X^T.$$

Криптограма складається з $(n\text{-}k)$ елементів [10] . Вектор e зберігає у собі інформацію, що прагнемо зашифрувати, тобто є інформаційним вектором. Інформаційний вектор додатково перетворюється за допомогою рівноважного кодування. Отримавши повідомлення, легітимний користувач, аналогічно з випадком криптосистеми Мак-Еліса, знімає дію маскуючих матриць і, використовуючи алгоритм швидкого декодування, отримує вектор e, що після рівноважного декодування представляє собою початково передану інформацію [11].

2.3. Нова гібридна криптосистема

Зважаючи на доведену стійкість розглянутих криптосистем (докладніше вона розглянута у наступному розділі), ми пропонуємо нову гібридну криптосистему, яка має ті ж переваги, що і її попередники, та навіть покращує їх показники. В основі пропонованої системи лежить поєднання принципів кодування інформації згідно із схемою Мак-Еліса та Нідеррайтера.

Секретними ключами гібридної схеми аналогічно першим двум схемам є матриця X (розмір $k \times k$ елементів), матриця P (розмір $n \times n$ елементів) та, у випадку недвійкового кодування, матриця D (розмір $n \times n$) [7, 11].

Відкритий ключ схеми – матриця $G_X = X \cdot G \cdot P \cdot D$, де G – породжуюча $k \times n$ матриця. З метою зашифрування інформаційний вектор розбивається на дві складові (I_1 та I_2). Після цього здійснюється формування криптограми:

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

При цьому перша складова інформації множиться на відкритий ключ $c_X = I_1 \cdot G_X$, як і у перетворенні згідно із схемою Мак-Еліса. Друга інформаційна складова I_2 перетворюється відповідно до схеми Нідеррайтера, а саме I_2 довжини m трансформується у закодований інформаційний вектор e довжиною n елементів (наприклад, за допомогою рівноважного кодування). Для утвореного вектору повинні виконуватися умови [7]:

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor m = \left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor$$

З метою забезпечення найбільшої стійкості рекомендується максимізувати вагу Хеммінга вектора e, оскільки тоді перебор всіх можливих значень цього вектору значно ускладнюється. Розшифрування у гібридній схемі відбувається, як і у схемі Мак-Еліса, що було описано у попередньому підрозділі, але з тією відмінністю, що інформація вилучається не тільки з вектору I, а ще й з вектору помилок e [12]. Цей факт дозволяє значно підвищити відносну швидкість передачі інформації, що докладішне буде розглянуто надалі .

3. Порівняльний аналіз криптосистем

Порівнюючи ефективність криптосистем, скористаємося такими чинниками, як відносна швидкість передачі інформаціїї, стійкість до класичного та квантового криптоаналізу, об'єм ключових даних, що потребує криптосистема, та довжина шифртексту відповідно до кожного варіанту.

3.1. Відносна швидкість передачі інформації

Спочатку розглянемо відносну швидкість передачі інформації. Вона характеризує ступінь використання в коді з виправленням помилок інформаційних можливостей двійкових послідовностей довжини n.

Оцінка відносної швидкості для схеми Мак-Еліса є найпростішою, оскільки відомо, що сформована за цим алгоритмом криптограма має довжину n, тоді як початковий інформаційний вектор має довжину k біт. Отже, відносна швидкість передачі у цьому випадку [13, 14] :

$$R = \frac{\log_2 2^k}{n} = \frac{k}{n}.$$

Відносна швидкість передачі інформації для схеми Нідеррайтера докладно розглянута у [7]. Згідно з цими даними вона становить

$$R = \frac{\left\lfloor \log_2 \left(\frac{n!}{t!(n-t)!} \right) \right\rfloor}{n-k}.$$

З використанням гібридної криптосистеми шифртекст, що формується, має довжину n, тоді як інформація кодується з поєднанням принципів Мак-Еліса та Нідеррайтера, розбиваю-

чи на дві складові I_1 та I_2, причому I_1 має довжину k біт, а I_2 перетворюється завдяки рівноважному кодуванню, тому максимально можлива прихована кількість біт визначається, як у схемі Нідеррайтера $\log_q\left(\sum_{i=0}^{t}(q-1)^i\frac{n!}{i!(n-i)!}\right)=n-k$. Тобто оцінку відносної швидкості передачі для гібридної криптосистеми можна зазначити як

$$R=\frac{k+\left\lfloor \log_2\left(\frac{n!}{t!(n-t)!}\right)\right\rfloor}{n}.$$

З наведених даних одразу можна зробити висновок, що з точки зору величини відносної швидкості гібридна система значно випереджає своїх попередників, за рахунок використання у кодуванні двох складових [7].

3.2. Стійкість до класичного криптоаналізу

Варто зазначити, що дослідниками було доведено, що стійкості криптосистем Мак-Еліса та Нідеррайтера еквівалентні. Продемонструємо це. Нехай відомо: синдром $c=e\cdot H_x$, тоді можна обчислити вектор $b=a\cdot E+e$, причому $c=b\cdot H_x$. У такому випадку b розглядають як шифртекст у системі Мак-Еліса. За умови, що знайдена атака зі складністю W для системи Мак-Еліса та відомо алгоритм для обчислення вектору a, який є секретною інформацією в схемі Мак-Еліса, вектор e, який містить секретну інформацію, у системі Нідеррайтера можна представити у вигляді $e=a\cdot E+b$, тобто складність визначення вектору e збігається зі складністю визначення вектора a. У протилежному випадку, коли існує ефективна атака на схемі Нідеррайтера, можливо, використовуючи у якості шифртексту вектор $(a\cdot E+e)\cdot \mathrm{D}^T=e\cdot \mathrm{D}^T$, обчислити вектори e та a. Варто зауважити, що з описаної вище точки зору слідує еквівалентність оцінок стійкості криптосистем Мак-Еліса та Нідеррайтера і гібридної криптосистеми [15].

Безпечність усіх трьох криптосистем заснована на нездатності вирішити такі фундаментальні проблеми теорії кодування, як загальна проблема декодування лінійних кодів та проблема знаходження кодового слова с заданною вагою.

Якщо розглядати можливість реалізації атак, варто згадати, що, незважаючи на те, що криптосистема Мак-Еліса, заснована на кодах Гоппа, досі вважається стійкою, як зазначав Роберт Мак-Еліс в своїй оригінальній статті, існує два основних шляхи, якими зловмисник може атакувати криптосистему [6]:

1. Зловмисник може спробувати відновити секретний ключ з відкритого ключа, а потім розшифрувати повідомлення.

2. Зловмисник може безпосередньо декодувати повідомлення, не вивчаючи структуру коду Гоппа.

Реалізацією подібного типу атак займається велика кількість дослідників, але досі не винайдено оптимальний ефективний варіант.

Також оцінку стійкості кожної з криптосистем до атак можна здійснити за допомогою визначення мінімальної кількості множин, що покривають усі помилки (кровельні множини). Їх кількість обчислюється згідно з формулою

$$N\geq\frac{C_n^t}{C_{n-k}^t}=\frac{\frac{n!}{t!(n-t)!}}{\frac{(n-k)!}{t!(n-k-t)!}}=\frac{n!(n-k-t)!}{(n-t)!(n-k)!}.$$

Причому $C_n^t = \frac{n!}{t!(n-t)!}$ представляє загальну кількість комбінацій помилок, а $C_{n-k}^t = \frac{(n-k)!}{t!(n-k-t)!}$ – максимальна кількість комбінацій помилок, які можуть бути покриті даною множиною [7]. Оцінка з цієї точки зору є певним чином заниженою, оскільки не враховується обчислювальна складність формування слів-кандидатів, що обчислюється відповідно до обраної множини.

3.3. Стійкість до квантового криптоаналізу

Нині існують різноманітні квантові алгоритми, серед яких найпопулярнішими є квантовий алгоритм Шора, квантовий алгоритм Гровера пошуку елемента в несортованій базі, квантові алгоритми криптоаналізу для перетворень в фактор-кільці та інші [16].

У ряді джерел зазначається, що квантовий алгоритм Шора не є ефективним для зламу безпеки криптосистеми Мак-Еліса. Найефективнішим квантовим алгоритмом по відношенню до кодової схеми Мак-Еліса є алгоритм Гровера. Він правильно розглядається не як через «базу даних», а як пошук коренів функції. З цієї точки зору варто розглянути застосування алгоритму Гровера в межах атаки декодування множини [17].

Алгоритм Гровера є загальним конструктивним перетворенням з умовних ланцюгів у квантові ланцюги знаходження коренів. Докладна реалізація квантової атаки декодування множини даних продемонстрована у [18, 19].

Варто відзначити, що базова атака декодування множини даних виконує пошук кореня функції випадковим чином. Пошук використовує приблизно в середньому $\frac{C_n^k}{0,29C_{n-t}^k} \approx c^{n/\lg n}$ проходів функції. Із застосуванням алгоритму Гровера ця оцінка трансформується у

$$\sqrt{\frac{C_n^k}{0,29C_{n-t}^k}} \approx c^{(1/2)n/\lg n}.$$

Кожна ітерація є квантовою функцією, що виконується за $O(n^3)$ кубітових операцій. Кожна ітерація також потребує часу $n^{O(1)}$ на квантовому комп'ютері розміру $n^{O(1)}$. Загальний час для знаходження S дорівнює $c^{(1/2+O(1))n/\lg n}$ на квантовому комп'ютері розміру $n^{O(1)}$. Знайшовши S, можна обчислити *m* та *e*, застосовуючи незначні додаткові зусилля [20].

Продемонструємо розглянуту інформацію щодо відносної швидкості передачі інформації та стійкості до обох видів криптоаналізу на прикладах, що наведені у табл. 1.

Таблиця 1

Залежність стійкості та відносної швидкості від виправляючої здатності коду

Параметри коду	Відносна швидкість передачі			Стійкість до класичного криптоаналізу, біт			Стійкість до квантового криптоаналізу, біт		
	М.	Н.	Г.	М.	Н.	Г.	М.	Н.	Г.
(2048,1828,41)	0,89	0,71	0,96	65,5			32	47,9	14,2
(2048, 1608,81)	0,78	0,63	0,92	90			44	49	26,7
(2048,1388, 121)	0,67	0,58	0,86	100			49	49	36
(2048,1168, 161)	0,57	0,54	0,8	100			48,7	48,1	42
(2048,948, 201)	0,46	0,51	0,74	92			44	47	46
(2048,728, 241)	0,35	0,49	0,67	78,9			38	46	49

Слід зауважити, що у таблиці використані такі позначення: М-криптосистема Мак-Еліса; Н-криптосистема Нідеррайтера; Г-гібридна криптосистема. Дані, що представлені у таблиці, крім стійкості до класичного криптоаналізу, оскільки для усіх трьох схем вона еквівалентна, задля кращого візуального сприйняття можна представити за допомогою графічного зображення (рис. 1, 2).

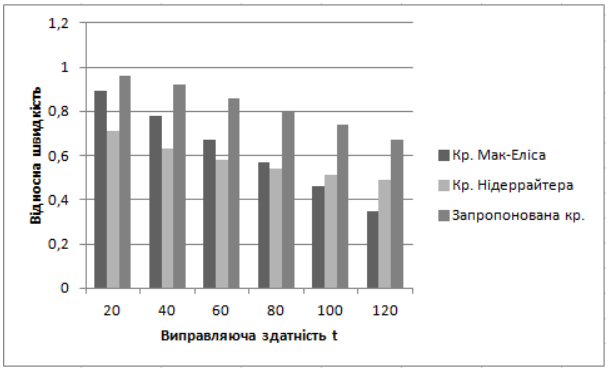

Рис. 1. Порівняння відносної швидкості передачі криптосистем

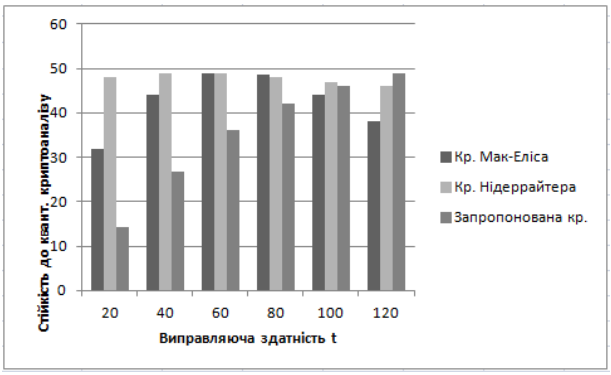

Рис. 2. Порівняння стійкості криптосистем до квантового криптоаналізу

Аналізуючи розглянуті дані, можна зробити висновок, що при однакових параметрах коду усі три криптосистеми забезпечують один і той же рівень стійкості до класичного криптоаналізу. Однак результати стійкості щодо квантового криптоаналізу різняться: стійкість до квантового криптоаналізу криптосистеми Мак-Еліса починає спадати після зниження відносної швидкості коду за межі 0,66. Очевидно, що збільшення виправляючої здатності гібридної криптосистеми і в той же час зі зменшенням відносної швидкості передачі, стійкість до квантвого криптоаналізу також зростає, але подальші дослідження продемонстрували, що ця тенденція зміниться за тієї ж умови, що впливає на стійкість схеми Мак-Еліса, а саме зниження відносної швидкості передачі інформації за межі 0,66.

3.4. Порівняння обсягу ключових даних та довжин шифртексту

Наступним кроком порівняємо об’єм ключових даних та довжини шифртексту, що формується відповідно до кожної з трьох криптосистем.

Оскільки у роботі розглядається двійковий випадок використання криптосистем, тому при оцінці обсягу ключових параметрів не буде враховано матрицю D, а також розгляд ведеться без врахування секретного поліному коду Гоппа.

Ключові параметри та спосіб формування шифртексту збігаються у випадку гібридної схеми та схеми Мак-Еліса, тому їх оцінки можна вважати еквівалентними. Секретний ключ цих схем складається з матриць X та P. Матриця X має розміри $k \times k$ елементів, а обсяг, який займає матриця P, визначається вектором перестановки з n елементів. Розмір відкритого ключа обох схем визначається матрицею $G_X = X \cdot G \cdot P$, розміром $k \times n$ елементів. Довжина сформованого шифртексту визначається згідно з довжиною криптограми $c_X^* = I_1 \cdot G_X + e$, що складається з n елементів. Отже, для криптосистеми Мак-Еліса та

гібридної криптосистеми довжина секретного ключа $l_{с.к.} = k \cdot k + n$, відкритого ключа $l_{в.к.} = k \cdot n$, а сформованого шифртексту $l_{ш.т} = n$. Звідси можна зазначити недолік криптосистем, що полягає у збільшеній довжині шифртексту відносно початкового інформаційного вектора. Відомо, що для криптосистеми Нідеррайтера секретним ключем є також матриці X та P. Розмір матриці P визначається, як і у попередньому випадку, але матриця X відрізняється і має розміри $(n-k)\times(n-k)$ елементів. Відкритим ключем цієї схеми є матриця $H_X = X \cdot H \cdot P$, що складається з $n\times(n-k)$ елементів. Довжина синдрому $s_X = e \cdot H_X^T$ при цьому дорівнює $(n-k)$.

Отже, для криптосистеми Нідеррайтера справедливі такі оцінки: обсяги секретного ключа $l_{с.к.} = (n-k)\cdot(n-k)+n$, обсяги відкритого ключа $l_{в.к.} = n\cdot(n-k)$, довжина шифр тексту $l_{ш.т} = n-k$.

Проаналізувавши наведену інформацію, можна зробити висновок, що обсяги секретного ключа у схемі Мак-Еліса та гібридній різняться з обсягами секретного ключа у схемі Нідеррайтера на $n^2 - 2\cdot n\cdot k$, різниця між сформованим шифртекстом дорівнює *k* елементів, але в той же час розміри відкритого ключа у схемі Нідеррайтера більші на n^2 елементів

Продемонструємо цей факт на прикладах, що відображено у табл. 2. Для розгляду різних рівнів безпеки було обрано параметри коду, що найчастіше зустрічаються у науковій літературі. Для більш наглядного розуміння представимо наведені у таблиці дані за допомогою гістограм (рис. 3 – 4).

Таблиця 2

Порівняння показників ефективності криптосистем

Криптосистема Мак-Еліса					
Параметри коду	Довжина ключів,біт	Довжина шифр тексту, біт	Відносна швидкість передачі	Стійкість до класичного криптоаналізу, біт	Стійкість до квантового криптоаналізу, біт
(1024,524,101)	812176	1024	0,51	54	25,8
(2048,1751,55)	6654097	2048	0,85	77	37,6
(4096,2584,253)	27754896	4096	0,88	128	62,6
(8192,6957,191)	105399785	8192	0,85	263	130
(16384,10322,867)	275675716	16384	0,63	636	310
Криптосистема Нідеррайтера					
Параметри коду	Довжина ключів, біт	Довжина шифр тексту, біт	Відносна швидкість передачі	Стійкість до класичного криптоаналізу, біт	Стійкість до квантового криптоаналізу, біт
(1024,524,101)	763024	500	0,57	54	26,7
(2048,1751,55)	698513	297	0,68	77	49
(4096,3604,83)	2261392	492	0,87	128	90,2
(8192,6957,191)	11650537	1235	0,84	263	166
(16384,10322,867)	136084036	6062	0,47	636	286
Гібридна криптосистема					
Параметри коду	Довжина ключів, біт	Довжина шифр тексту, біт	Відносна швидкість передачі	Стійкість до класичного криптоаналізу, біт	Стійкість до квантового криптоаналізу, біт
(1024,524,101)	812176	1024	0,79	54	24,2
(2048,1751,55)	6654097	1945	0,95	77	18,9
(4096,3604,83)	27754896	3892	0,95	128	31,8
(8192,6957,191)	105399785	7618	0,93	263	77
(16384,10322,867)	275675716	13107	0,8	636	267

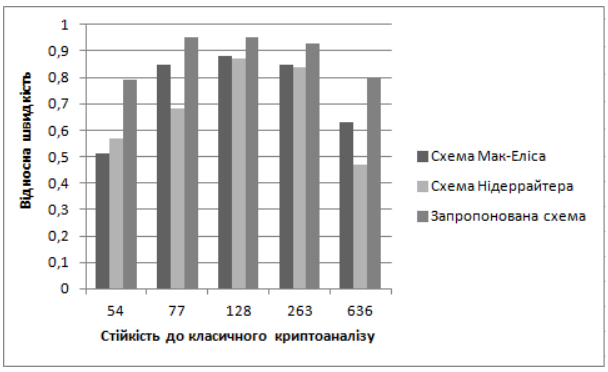

Рис. 3. Залежність між відносною швидкістю та стійкістю криптосистем

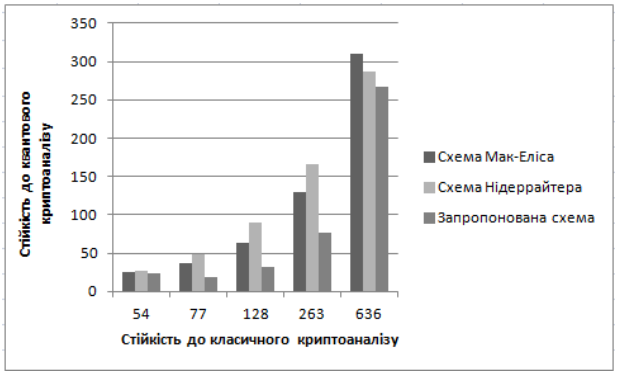

Рис. 4. Залежність між величиною стійкості до класичного та квантового криптоаналізу

Проаналізувавши наведені дані, можна зробити висновок, що для забезпечення аналогічного рівня стійкості до квантового криптоаналізу, порівняно зі звичайним криптоаналізом (наприклад, порівнюючи показники для параметру коду n=16384 n=8192), необхідно збільшити обсяги ключових даних більше, ніж у три рази. Також варто відзначити, що стійкість криптосистем до квантового криптоаналізу безпосередньо залежить від показників їх відносної швидкості.

Через перевагу в останньому показнику гібридна криптосистема показала продемонстрували результати у стійкості до квантового криптоаналізу, але зменшення стійкості не є критичним, порівняно з іншими схемами. На жаль, однозначно визначити, яка з трьох криптосистем забезпечує найкращий захист, неможливо, оскільки дані для різних наборів параметрів кодів будуть різнитися.

Однак, очевидною перевагою гібридної криптосистеми, про яку варто нагади, в контексті розгляду ефективності криптосистем, є те, що вона дозволяє шифрувати більший об'єм інформації з використанням того ж об'єму ключів, при цьому забезпечуючи належний рівень захисту.

Висновки

Проаналізувавши весь спектр інформації, що стосується кодових криптосистем, можна зробити ряд висновків.

По-перше, дослідження виявили, що використання алгебраїчних кодів у контексті постквантової криптографії є дуже перспективним напрямком, оскільки вони дозволяють забезпечити високу швидкість криптоперетворення, контроль помилок, що можуть відбутися у каналі зв'язку, а також стійкість до класичного та квантового криптоаналізу. У зв'язку з наявністю згаданих переваг у використанні кодів з метою побудування алгоритмів постквантової криптографії було запровоновано новий, так званий гібридний алгоритм, що поєднує принципи зашифрування згідно з криптосистемами Мак-Еліса та Нідеррайтера.

У свою чергу, подальший порівняльний аналіз всіх трьох криптосистем виявив, що використовуючи запропоновану схему, ключові дані займають ті ж обсяги, що і ключові дані

криптосистеми Мак-Еліса, і формуються за аналогічний час, при цьому дозволяючи забезпечити більшу відносну швидкість передачі і аналогічну стійкість до криптоаналізу. Единим недоліком є збільшений час розшифрування за рахунок додання вилучення інформації, як у схемі Нідеррайтера, але збільшення цього показника не є критичним.

Незважаючи на продемонстровані переваги для усіх криптосистем залишається відкритим питання зменшення обсяги використовуваних ключових даних, які, в умовах використання квантових комп'ютерів для забезпечення стійкості, ще потрібно буде збільшити в рази. Даний напрямок залишається актуальним вектором дослідження в лоні сучасної криптографії.

Список літератури:

1. Menezes A.J., P.C. van Oorschot, Vanstone S.A. // Handbook of Applied Cryptography. CRC Press, 1997. – 794 p.

2. Ferguson N. and Schneier B. Practical Cryptography. – John Wiley & Sons, 2003. – 432 p.

3. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future // The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. [On-line]. Available: https://pqcrypto2016.jp

4. Koblitz N. and Menezes A.J. A Riddle Wrapped in an Enigma. [On-line] Available: https://eprint.iacr.org/2015/1018.pdf

5. MacWilliams F. J. and Sloane N. J. A. The theory of error-correcting codes. North-Holland, Amsterdam, New York, Oxford, 1977. – 762 p.

6. McEliece R. J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report 42-44, Jet Propulsion Lab., January-February, 1978. – P. 114-116.

7. Kuznetsov A., Svatovskij I., Kiyan N. and Pushkar'ov A. Code-based public-key cryptosystems for the post-quantum period. 2017 // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkov, 2017. – P. 125-130.

8. Finiasz M. and Sendrier N. Security bounds for the design of codebased cryptosystems // M. Matsui, ed., Advances in Cryptology, ASIACRYPT. – 2009. – Vol. 5912 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009. – P. 88 -105.

9. Courtois N., Finiasz M. and Sendrier N. How to achieve a McEliece-based digital signature scheme // Advances in Cryptology – ASIACRYPT. – 2001. – Vol. 2248. – P. 157–174.

10. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory. – 1986. – Vol. 15. – P. 19-34.

11. Kuznetsov A., Pushkar'ov A., Kiyan N. and Kuznetsova T. Code-based electronic digital signature // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018. – P. 331-336.

12. Kuznetsov A., Lutsenko M., Kiian N., Makushenko T. and Kuznetsova T. Code-based key encapsulation mechanisms for post-quantum standardization // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kyiv, Ukraine, 2018. – P. 276-281.

13. Kuznetsov A., Kiian A., Lutsenko M., Chepurko I. and Kavun S. Code-based cryptosystems from NIST PQC // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kyiv, Ukraine, 2018. – P. 282-287.

14. Sidelnikov V. M. and Shestakov S. O. On insecurity of cryptosystems based on generalized Reed-Solomon codes // Discrete Mathematics and Applications. – 1992. – p. 439-444.

15. Yuan Xing Li, R. H. Deng and Xin Mei Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems // IEEE Transactions on Information Theory. – Jan. 1994. – Vol. 40, no. 1. – P. 271-273.

16. Bernstein D., Buchmann J. and Dahmen E. Post-Quantum Cryptography. – Springer-Verlag, Berlin-Heidleberg, 2009. – 245 p.

17. Proos J. and Zalka C. 2003. Shor's discrete logarithm quantum algorithm for elliptic curves // Quantum Info. Comput. – 3, 4 (July 2003). – P. 317-344.

18. Bernstein D.J., Lange T., Peters C. Attacking and Defending the McEliece Cryptosystem // Buchmann J., Ding J. (eds) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science. – Vol. 5299. Springer, Berlin, Heidelberg. – pp 31-46.

19. Grover L. A fast quantum mechanical algorithm for database search // Proceedings of the 28th annual ACM symposium on the theory of computing (STOC, 96). – ACM Press, New York, 1996. – P. 212-219.

20. Sendrier N. Decoding one out of many // Yang, B.Y., ed.: PQCrypto 2011. – Vol. 7071 of LNCS. Springer, 2011. – P. 51-67.

Харківський національний
університет імені В.Н.Каразіна;
АТ «Інститут інформаційних технологій», Харків

Надійшла до редколегії 05.11.2018