УДК 004.056.55 DOI: 10.30748/soi.2018.153.16

С.П. Євсєєв, О.С. Циганенко

Харківський національний економічний університет ім. С. Кузнеця, Харків

РОЗРОБКА НЕСИМЕТРИЧНОЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ НІДЕРРАЙТЕРА НА МОДИФІКОВАНИХ ЕЛІПТИЧНИХ КОДАХ

Розглядаються способи модифікації лінійних блокових кодів (еліптичних кодів) для побудови крипто-кодових конструкцій. Детально розглянуто метод модифікації шляхом укорочення. Запропоновано математичну модель модифікованої несиметричної крипто-кодової системи (МНККС) Нідеррайтера на еліптичних кодах. Пропонуються прикладні алгоритми формування та розшифрування криптограми в МНККС на основі модифікованих крипто-кодових конструкцій. Розроблена блок-схема алгоритмів формування та розшифрування криптограми в МНККС Нідеррайтера на основі модифікованих крипто-кодових конструкцій з урахуванням особливостей реалізації. Проведено дослідження властивостей модифікованої НККС Нідеррайтера: досліджено залежність складності формування криптограми, складності розкодування криптограми, складності злому та складності кодування. За результатами досліджень, не зважаючи на зменшення потужності поля після модифікації для МНККС, характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційної НККС Нідеррайтера. Таким, чином розглянута МНККС Нідеррайтера є конкурентоздатною системою забезпечення основних послуг безпеки та є перспективним напрямком досліджень по зниженню енерговитрат крипто-перетворень в ККС з використанням кодових конструкцій, шляхом їх модифікації.

Ключові слова: *несиметричні крипто-кодові системи, модифіковані крипто-кодові конструкції, укорочені коди, Нідеррайтер.*

Вступ

Постановка проблеми. Швидке зростання обсягів оброблюваних даних та розвиток обчислювальної техніки висувають нові вимоги до надійності та забезпечення безпеки даних. Проведені дослідження в області впливу квантових обчислень, що використовують явища квантової суперпозиції та квантової заплутаності для передачі та обробки даних, показали, що квантові комп'ютери, які використовують спеціальні алгоритми (наприклад, алгоритм Шора), будуть здатні до факторизації чисел за поліноміальний час [15; 17]. Отже, криптографічні системи *RSA*, *ECC*, *DSA* будуть вразливі до атак "грубої сили" (*brute force attacks*) з використанням повномасштабного квантового комп'ютера. Тому основні дослідження і розробки криптографічних засобів захисту інформації (КЗЗІ) в нинішній час спрямовані на пошуки рішень, що не мали б вразливостей щодо квантових обчислень і були б одночасно стійкими до атак за допомогою звичайних комп'ютерів. Такі алгоритми відносяться до розділу квантово-стійкої криптографії (*quantum safe cryptography* або *quantum resistant cryptography*) [8]. Через швидку появу нових схем не приділяється достатня увага давно відомим, несиметричним крипто-кодовим системам (НККС) на основі ТКС Мак-Еліса і Нідеррайтера, що також є квантово-стійкими.

Аналіз останніх досліджень і публікацій [1–14; 16; 18] показав, що використання класичних теоретико-кодових схем Мак-Еліса і Нідеррайтера можливо тільки при зменшенні енергетичних витрат на їх практичну реалізацію зі збереженням рівня криптостійкості криптосистеми в цілому. Тому перспективним напрямком досліджень є зниження енерговитрат криптоперетворень в ККС з використанням кодових конструкцій, шляхом їх модифікації.

Метою статті є розробка математичного апарату та практичних алгоритмів модифікованої несиметричної крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах.

Основними завданнями дослідження визначено такі:

розробка математичної моделі модифікованої НККС Нідеррайтера;

розробка практичних алгоритмів модифікованої НККС Нідеррайтера;

дослідження властивостей модифікованої НККС Нідеррайтера.

Розробка математичної моделі модифікованої НККС Нідеррайтера

Відомі способи модифікації лінійних блокових кодів найдокладніше розглянуті в [3; 5–6; 16]. На рис. 1 наведені найбільш поширені способи модифікації. Подовження (n, k, d) лінійного блокового коду полягає в збільшенні довжини n + x шляхом додавання нових інформаційних символів k + x. Розширення (n, k, d) лінійного блокового коду полягає в збільшенні довжини n + x шляхом додавання нових перевірочних символів r + x.

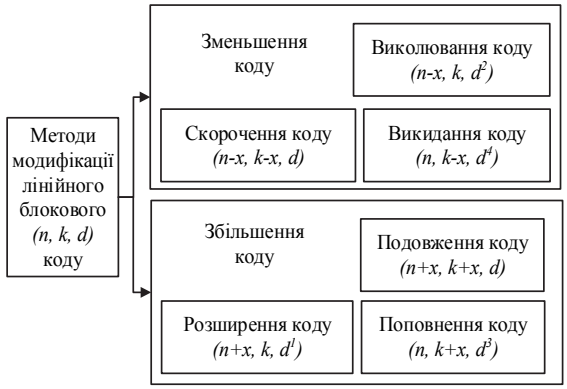

Рис. 1. Способи модифікації блокових кодів

Виколювання (*n, k, d*) лінійного блокового коду полягає в зменшенні довжини n – x шляхом зменшення перевірочних символів r – x. *Скорочення* (*n, k, d*) лінійного блокового коду полягає в зменшенні довжини n – x шляхом зменшення інформаційних символів k – x. *Поповнення* (*n, k, d*) лінійного блокового коду полягає в збільшенні довжини інформаційних символів k + x без збільшення довжини коду. *Викидання* (*n, k, d*) лінійного блокового коду полягає в зменшенні інформаційних символів k – x без збільшення довжини коду.

Потенційна стійкість НККС визначається складністю декодування випадкового (n, k, d) блокового коду. Отже, для побудови потенційно стійких крипто-кодових конструкцій необхідно використовувати способи модифікації, що не допускають зниження мінімального кодової відстані. Способи подовження і укорочення лінійних блокових кодів не змінюють мінімальну відстань, і тому дозволяють будувати стійкі до злому НККС [5–6; 13; 16].

Найбільш простий і зручний спосіб модифікації лінійного блокового коду, що не зменшує мінімальну кодову відстань, полягає у укороченні його довжини шляхом скорочення інформаційних символів. Нехай $I=(I_1, I_2, \ldots, I_k)$ – інформаційний вектор (n, k, d) блокового коду. Визначимо підмножину h інформаційних символів, $|h|=x$, $x \le 1/2k$. Помістимо в інформаційний вектор I в підмножину h нулі, тобто $I_i=0$, $\forall I_i \in h$. На інших позиціях вектора I помістимо інформаційні символи. При кодуванні інформаційного вектора символи множини h не беруть участь (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на x кодових символів. Для модифікації (укорочення) еліптичних кодів будемо використовувати зменшення набору точок кривої [1–2].

Розглянемо формальний опис математичної моделі НККС Нідеррайтера, яка модифікована шляхом укорочення вектора помилки, що сформований на основі рівноважного кодування. Математична модель задається сукупністю таких елементів [9]:

– множина відкритих текстів $M=\left\{M_1, M_{2,}\ldots M_{q^k}\right\}$, де $M_i=\left\{e_0, e_{h_1,}\ldots e_{h_k}, e_{e-1}\right\}$, $\forall e_e \in GF(q)$; h_e – символи вектора помилки, що дорівнюють нулю, $|h|=\frac{1}{2}e$, тобто $e_i=0$, $\forall e_i \in h$;

– множина закритих текстів $S=\left\{S_0, S_1, \ldots S_{q^r}\right\}$, де $S_i=\left\{S^*_{X_0}, S^*_{h_1}, \ldots S^*_{h_j}, S^*_{X_r}\right\}$, $\forall S_{X_r} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа – перевірочної матриці еліптичного коду (ЕС): $\varphi=\left\{\varphi_1, \varphi_2, \ldots, \varphi_r\right\}$, де $\varphi_i : M \to S_{r-h_e}$, $i=1,2,\ldots,e$ – множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування). $\varphi^{-1}=\left\{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_r^{-1}\right\}$, де $\varphi_i^{-1} : S_{r-h_e} \to M$, $i=1,2,\ldots,e$.

– множина ключів, які параметризують прямі відображення (відкритий ключ уповноваженого користувача):

$$KU_{a_i}=\left\{KU_{1_{a_i}}, KU_{2_{a_i}}, \ldots, KU_{r_{a_i}}\right\}=$$
$$=\left\{H^{EC1}_{X_{a_i}}, H^{EC2}_{X_{a_i}}, \ldots, H^{ECr}_{X_{a_i}}\right\},$$

де $H^{EC_i}_{X_{a_i}}$ – перевірочна r×n матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами GF(q), тобто $\varphi_i : M \xrightarrow{KU_{i_{a_i}}} S^*_{r-h_e}$, $i=1,2,\ldots,e$, a_i – набір коефіцієнтів многочлена кривої $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, однозначно задає конкретний набір точок кривої з простору P^2;

– множина ключів, які параметризують обернені відображення (особистий (закритий) ключ уповноваженого користувача):

$$KR=\left\{KR_1, KR_2, \ldots, KR_r\right\}=\left\{\begin{matrix}\left\{X,P,D\right\}_1,\\ \left\{X,P,D\right\}_2, \ldots, \left\{X,P,D\right\}_r\end{matrix}\right\},$$

$\left\{X,P,D\right\}_i=\left\{X^i, P^i, D^i\right\}$, де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами зі GF(q); P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з GF(q); D^i – діагональна сформована джерелом ключів матриця з елементами з GF(q), тобто $\varphi_i^{-1} : S^*_{r-h_e} \xrightarrow{KR_i} M$, $i=1,2,\ldots,s$. Складність виконання оберненого відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язанням теоретико-складної задачі декодування випадкового коду (коду загального положення).

Вихідними даними при описі розглянутої несиметричною крипто-кодової системи захисту інформації є:

– недвійковий рівноважний код над GF(q), тобто множина послідовностей довжини n та ваги $w(\varepsilon_i)$;

– алгеброгеометричний блоковий (n, k, d) код C над GF(q), тобто така множина кодових слів $C_i \in C$, що виконується рівність $C_i H^T = 0$, де H – перевірочна матриця алгеброгеометричного блокового коду;

– IV – вектор ініціалізації, IV= |h| =½ де – елементи скорочення (h_e – символи вектора помилки, рівні нулю, |h|=1/2e, тобто $e_i = 0$, $\forall\ e_i \in h$);

– маскуючі матричні відображення, задані множиною матриць $\{X, P, D\}_i$, де X – невироджена $k \times k$ матриця над GF(q), P – перестановочна $n \times n$ матриця над GF(q) з одним ненульовим елементом в кожному рядку і в кожному стовпці матриці, D – діагональна $n \times n$ матриця над GF(q) з ненульовими елементами на головній діагоналі;

– r – деякий параметр $r \in_R Z_{q^m}$, $Z_{q^m} = \left\{0,1,...2^n - 1\right\}$,

n – деякий параметр $n \in_R Z_{q^n}$, $Z_{q^n} = \left\{1,...2^n\right\}$;

На основі рівноважного кодування формується закритий текст $C_j \in C$ за введеним відкритим текстом $M_i \in M$ і заданим ключем H_X^{ECu}, $u \in \{1,2,...,s\}$. Це здійснюється шляхом формування синдромної (в термінах завадостійкого кодування) послідовності S_{X_j}, що відповідає рівноважній послідовності $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$:

$$S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \times \left(H_X^{ECu}\right)^T,$$ причому вага Гемінга (кількість ненульових елементів) вектора e не перевищує виправної здатності використовуваного алгебраїчного блокового (n,k,d) коду:

$$\forall i : 0 \le w\left(M_i\right) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Потужність множин M та C визначається допустимим спектром ваг $w\left(M_i\right)$, тобто в загальному випадку (для всіх допустимих значень $w\left(M_i\right)$) маємо:

$m = \sum_{i=0}^{t} (q-1)^i \times C_n^i$, де C_n^i – біноміальний коефіцієнт, $C_n^i = \frac{n!}{i! \cdot (n-1)!}$.

Найбільш доцільно величину $w\left(M_i\right)$ вибирати відповідно до необхідного значенням безпеки передачі інформації. Тоді для $w\left(M_i\right) = \text{const} = w(e)$ маємо: $m = (q-1)^{w(e)} \times C_n^{w(e)}$, а послідовність $M_i = \{e_0, e_1, ..., e_{n-1}\}$ з множини $M = \{M_1, M_2, ..., M_m\}$ формується як результат деякого відображення ψ, реалізованого шляхом надлишкового кодування недвійковими рівноважними кодами ненадлишкових інформаційних послідовностей.

Сформований закритий текст $C_j \in C$ однозначно відповідає вектору $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Сформуємо вектор ініціалізації IV=EC–h_j, де h_j – інформаційні символи, що дорівнюють нулю, $|h| = \frac{1}{2}k$, тобто. $I_i = 0$, $\forall\ I_i \in h$.

Формування укороченого вектора помилки e_x=e(A) – IV.

Відкритий ключ формується шляхом множення перевірочної матриці алгеброгеометричного коду на матриці маскування:

$$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u,\ u \in \{1,2,...,s\},$$

де H^{EC} – перевірочна $n \times (n-k)$ матриця алгеброгеометрического блокового (n,k,d) коду з елементами з GF(q).

В канал зв'язку поступає синдромна послідовність $S^*_{r-h_e} = \left(e_n - h_e\right) \times H_X^{EC^T}$.

На стороні прийому уповноважений користувач, який знає маскування (набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) і вектори ініціалізації (кількість і місця нульових символів вектора помилки) формує кодову послідовність як одне (будь-яке) з можливих рішень рівняння:

$$S^*_{r-h_e} = c^*_{X_i} \cdot H^T_{X_j},$$

тобто знаходить такий вектор $c^*_{X_i}$, який розкладається на суму: $c^*_{X_i} = c_{X_i} + M_i$, де c_{X_i} – одне (будь-яке) з можливих кодових слів замаскованого коду з перевірочної матрицею $H^T_{X_j}$, тобто $c_{X_i} \times H^T_{X_j} = 0$.

Далі уповноважений користувач, використовуючи набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$, формує вектор: $\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$, тобто демаскує кодову послідовність $c^*_{X_i}$.

Після підстановки отримаємо рівність:

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(c_{X_i} + M_i\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= c_{X_i} \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

Уповноважений користувач, який сформував вектор, має можливість застосувати швидкий (поліноміальної складності) алгоритм завадостійкого декодування і сформувати таким чином вектор $\bar{c}^{*} = c_X^{*} \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$ та вектор $M_i^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$.

Для відновлення інформаційної рівноважної послідовності M_i достатньо знову помножити вектор M_i^u на матриці маскування D^u та P^u, але в іншому порядку:

$$M_i = M_i^u \cdot P^u \cdot D^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u = M_i .$$

Формування шуканого вектора помилки e:

$$M = M_i + IV.$$

При розшифруванні криптограми (після отримання вектора помилки, перед використанням алгоритму рівноважного кодування) для отримання інформації вводяться “нульові” символи укорочення.

Розробка практичних алгоритмів модифікованої НККС Нідеррайтера

Таким чином, усі сформульовані науково-прикладні висновки підтверджено результатами експерименту.

Алгоритм формування криптограми в модифікованій НККС Нідеррайтера представимо у вигляді послідовності кроків (рис. 2):

Крок 1. Введення інформації, яка підлягає кодуванню. Введення відкритого ключа H_X^{EC}.

Крок 2. Формування вектора помилки e, вага якого не перевищує $\le t$ – виправляє здатність еліптичного коду на основі алгоритму недвійковий рівноважного кодування.

Крок 3. Формування укороченого вектора помилки: e_x=e(A) – IV.

Крок 4. Формування кодограми:

$$S^{*}_{r-h_e} = \left(e_n - h_e\right) \times H_X^{EC^T} .$$

Алгоритм розкодування кодограми в модифікованій НККС Нідеррайтера представимо у вигляді послідовності кроків (рис. 3):

Крок 1. Введення кодограми S_X, що розкодовується.

Введення закритого ключа – матриць X, P, D.

Крок 2. Знаходження одного з можливих рішень рівняння $S^{*}_{r-h_e} = \bar{c}^{*} \times \left(H_X^{EC}\right)^T$.

Крок 3. Зняття дії діагональної і переставної матриць: $\bar{c}^{*} = c_X^{*} \cdot D^{-1} \cdot P^{-1}$.

Крок 4. Розкодування вектора $\bar{c}^{*}$. Формування вектора e_x’.

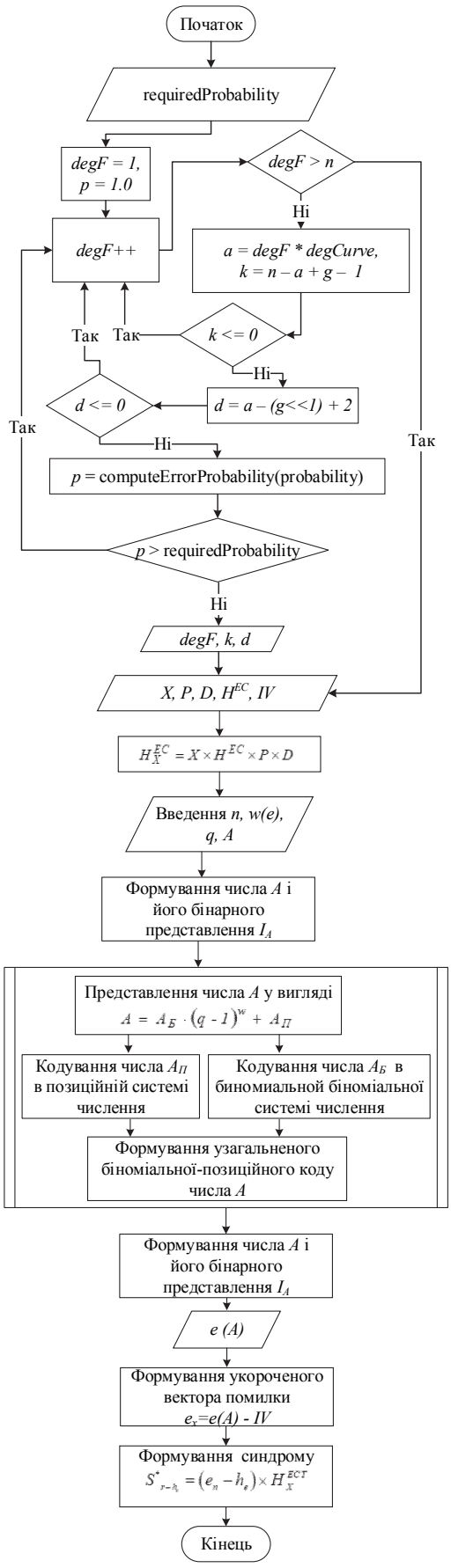

Рис. 2. Алгоритм формування кодограми в МККС Нідеррайтера на МЕС

Крок 5. Перетворення вектора e_x'

$$e_x = e_x' \times P \times D.$$

Крок 6. Формування шуканого вектора помилки e: $e = e_x + IV$.

Крок 7 Перетворення вектора e на основі використання недвійковий рівноважного коду в інформаційну послідовність.

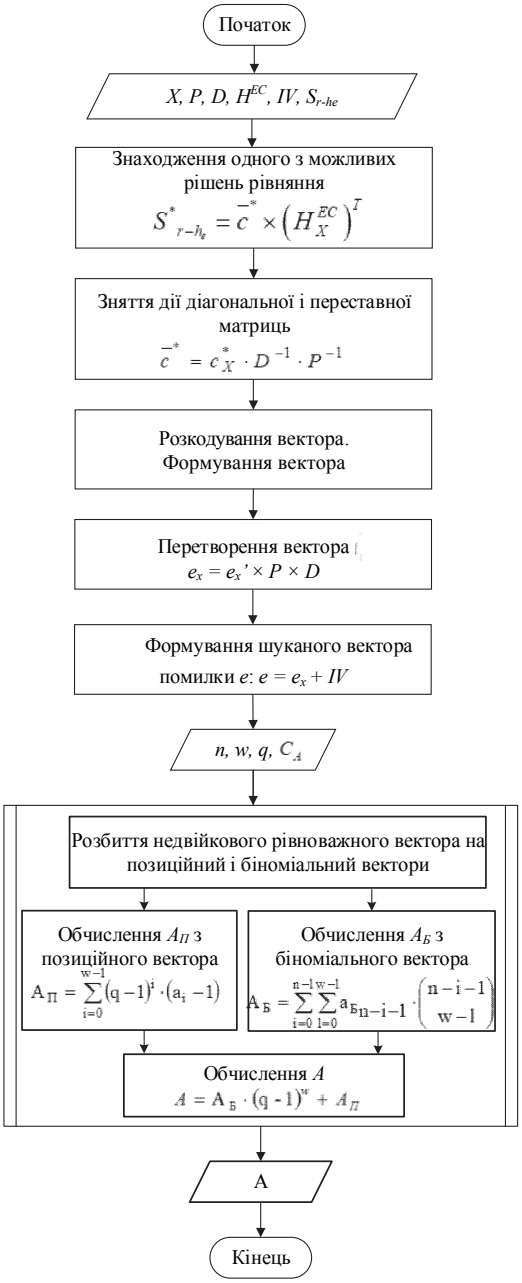

Рис. 3. Алгоритм розкодування кодограми в МККС Нідеррайтера на МЕС

Порівняльне оцінювання параметрів МНККС Нідеррайтера з використанням модифікованих еліптичних кодів

Введемо такі позначення:

l_I – довжина інформаційної послідовності (блока), яка надходить на вхід ККС схеми (в бітах); l_K – довжина відкритого ключа (в бітах); l_{K+} – довжина закритого ключа (в бітах); l_S – довжина кодограми (в бітах); O_K – складність формування кодограми (кількість групових операцій); O_{SK} – складність розкодування кодограми (кількість групових операцій); O_{K+} – складність розв'язання задачі аналізу (кількість групових операцій); L_0 – довжина вихідного тексту; uk – НККС з укороченими модифікованими еліптичними кодами (МЕС).

У табл. 1 і на рис. 4 наведені результати досліджень складності формування криптограми в різних GF(2^m).

Таблиця 1

Залежність складності формування криптограми в різних GF(2^m)

GF(2^m)		3	4	5	6	7	8	9	10
R	0.5	817	2140	8706	10722	83000	207422	710920	**52704**
	0.75	968	6282	11461	60760	210170	605005	1018079	**103822**
	0.5 (uk)	817	2140	8706	**10722**	83000	207422	710920	4572881
	0.75 (uk)	968	6282	11461	**60760**	210170	605005	1018079	5561379

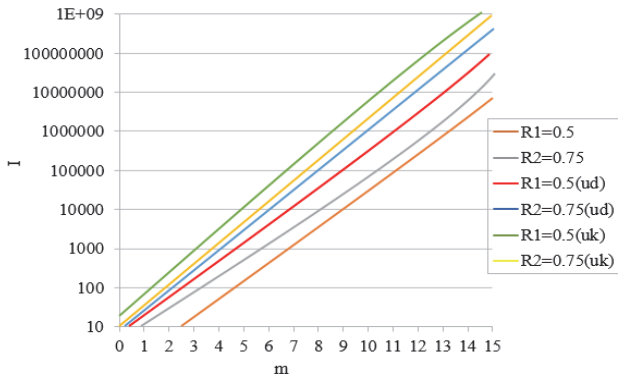

Рис. 4. Залежність складності формування криптограми в різних GF(2^m)

Аналіз результатів розрахунків свідчить про зростання швидкості формування криптограми при використанні укорочених МЕС.

Довжина кодограми (в бітах) визначається за таким виразом:

$$l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m.$$

У табл. 2 і на рис. 5 наведені результати досліджень складності розкодування криптограми в різних GF(2^m).

Таблиця 2

Результати досліджень складності розкодування криптограми в різних GF(2^m)

GF(2^m)		3	4	5	6	7	8	9	10
R	0.5	120	680	2092	12397	127523	1203984	10637991	**175645127**
	0.75	640	2378	7512	61246	136495	1494284	12768954	**193648924**
	0.5 (uk)	1280	11028	78634	**760553**	4566721	12948312	92516734	1.00E+09
	0.75 (uk)	5127	23674	277830	**5220573**	19768512	52694229	10637991	175645127

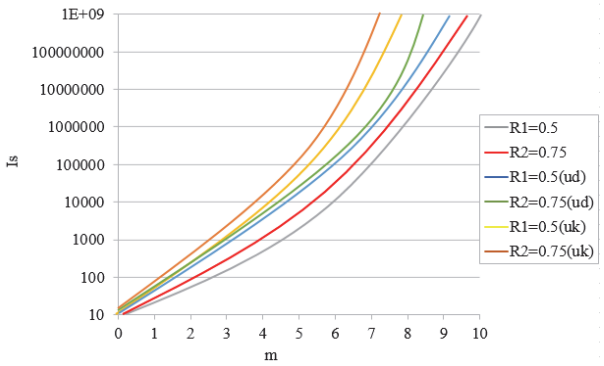

Рис. 5. Залежність складності розкодування криптограми в різних GF(2^m)

Аналіз табл. 1–2, рис. 4–5 показав, що в подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування (≈ в 3 разів) і розкодування (≈ в 5 разів) криптограми.

У табл. 3 і на рис. 6 наведені результати досліджень складності злому алгоритмом переставного декодування в різних GF(2^m).

Складність формування кодограми визначається виразами:

– для укорочених МЕС: при реалізації систематичного кодування визначається виразом:

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right);$$

для несистематичного кодування:

$$O_K = O_K = (k+1)\times(k+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+ +O\left(\frac{1-K_C^u}{K_f}\times L\right).$$

Таблиця 3

Залежність складності злому над GF(2^m)

GF(2^m)		3	4	5	6	7	8	9	10
R	0.5	2.868	4.843	6.22	7.891	8.995	10.37	11.74	**13.19**
	0.75	4.867	6.613	8.03	12.245	13.13	15.16	17.18	**19.23**
	0.5 (uk)	8.234	12.647	14.742	**18.767**	21.102	24.05	27.002	29.95
	0.75 (uk)	9.764	13.32	16.892	**19.76**	22.93	26.11	29.302	32.484

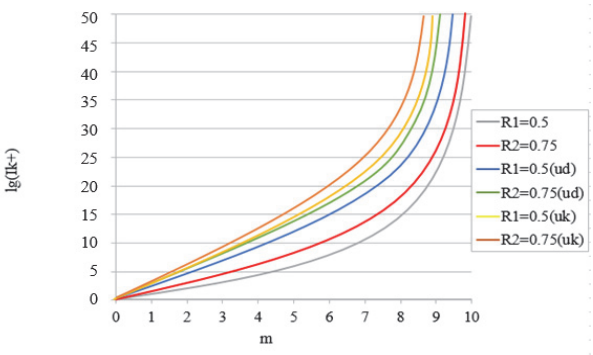

Рис. 6. Залежність складності злому над GF(2^m) (переставне декодування)

Аналіз рис. 6 показав, що зменшення потужності поля до 2^6 не привело до істотного зниження складності злому криптограми методом переставного декодування.

Складність формування кодограми визначається виразами:

– укорочених МЕС: для систематичного та несистематичного кодування визначається виразами:

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right);$$

$$O_K = O_K = (k+1)\times(k+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+ +O\left(\frac{1-K_C^u}{K_f}\times L\right).$$

Складність вирішення завдання аналізу (декодування) визначимо виразом:

$$O_{K+} = N_{\text{покр}}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r+N_F \text{ або } (N_K);$$

Складність розкодування кодограми визначається такими виразами:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k\right)^2+1/2k^2+4t^2+ +\frac{\left(t^2+t-2\right)^2}{4}+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right).$$

У табл. 4 і на рис. 7 наведені результати досліджень складності злому і складності кодування для різних швидкостей R в різних GF(2^m).

Таблиця 4

Складність злому і складності кодування для різних швидкостей R

lg(ls)		3	4	5	6	7	8	9	10
R	0.5	18.22	21.42	38.77	54.13	82.14	165.84	358.33	**672.37**
	0.75	33.17	51.75	61.09	78.37	83.72	179.13	371.09	**684.94**
	0.5 (uk)	56.88	78.92	94.91	**120.83**	182.39	276.27	459.81	783.46
	0.75 (uk)	58.03	80.52	104.56	**128.79**	189.74	287.33	476.52	794.28

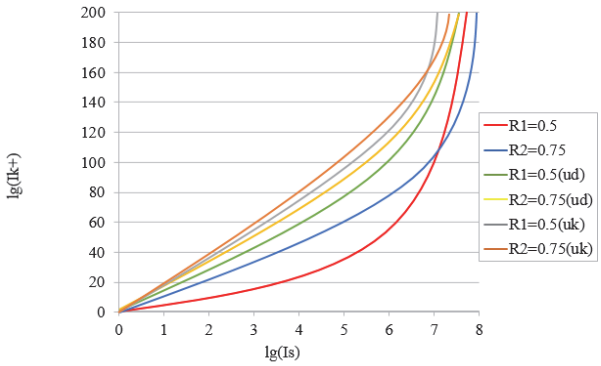

Рис. 7. Зведена діаграма складності злому і складності кодування

У табл. 5 і на рис. 8 наведені залежності обсягу відкритих ключових даних для різних показників стійкості.

Таблиця 5

Залежності обсягу відкритих ключових даних для різних показників стійкості

lg(l_k+)		5	20	35	50
R	0.5	30	2278137	**12329538**	22541273
	0.75	87	4351076	**14097276**	77520337
	0.5(uk)	968	1034682	**6126273**	8602376
	0.75(uk)	799	1897092	**6832018**	7027160

Аналіз наведених результатів табл. 4–5 та рис. 7–8 ясно демонструє, за рахунок чого отримано зростання відносної швидкості передачі даних: обсяг ключових даних в системах на укорочених кодах вдвічі менший за класичну НККС.

У табл. 6 наведені результати досліджень ємнісний характеристики при програмної реалізації від потужності поля.

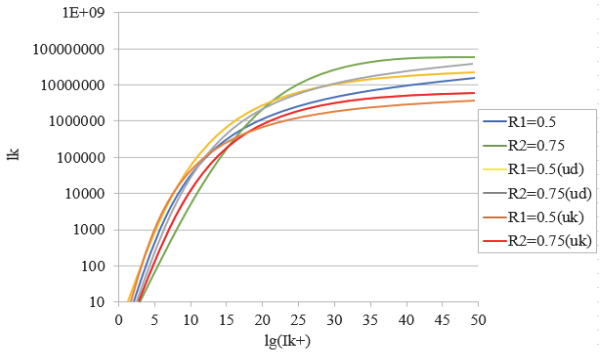

Рис. 8. Залежності обсягу відкритих ключових даних для різних показників стійкості

Таблиця 6

Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

Криптосистеми	2^5	2^6	2^7	2^8	2^9	2^{10}
НККС Нідеррайтера на ЕС	1×10^7	$1{,}8\times10^7$	$3{,}2\times10^7$	$4{,}7\times10^7$	$6{,}3\times10^7$	$\mathbf{8{,}2\times10^7}$
МНККС Нідеррайтера на укорочених МЕС	1×10^7	$\mathbf{1{,}7\times10^7}$	$2{,}9\times10^7$	$4{,}4\times10^7$	$6{,}2\times10^7$	8×10^7

Результуюча табл. 6 показує кількість групових операцій програмної реалізації НККС залежно від потужності поля. Видно, якщо для реалізації НККС Нідеррайтера в GF(2^{10}) необхідно 82,5 × 10^6 групових операцій, то реалізація МНККС на укорочених МЕС в GF(2^6) вимагає 17,7 – 18,6 × 10^6 групових операцій, тобто в 4,5 рази менше.

Висновки

Запропоновано формальний опис математичної моделі модифікованої крипто-кодової конструкції на основі НККС Нідеррайтера на МЕС, практичні алгоритми її реалізації (шифрування та розшифрування), основною відмінністю є зниження обсягу переданих даних шляхом укорочення вектору помилки перед формуванням синдрому на стороні відправника у класичній НККС Нідеррайтера, що дозволяє знизити потужність поля і відповідно енергетичні витрати. Таким, чином розглянута МНККС Нідеррайтера на МЕС формується над полем GF(2^6) та дозволяє є конкурентоздатною системою забезпечення основних послуг безпеки та є перспективним напрямком досліджень по зниженню енерговитрат криптоперетворень в ККК на основі МНККС Нідеррайтера на МЕС.

Список літератури

1. Алгоритмические основы эллиптической криптографии / А.А. Болотов и др. – М.: МЭИ, 2000.

2. Мищенко В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский. – Минск: Энциклопедикс, 2007.

3. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции "Московский университет и развитие криптографии в России". – МГУ, 2002, С. 1-22.

4. Грищук Р.В. Основи кібернетичної безпеки: Монографія; за заг. ред. Ю.Г. Данника / Р.В. Грищук, Ю.Г. Даник. – Житомир: ЖНАЕУ, 2016.

5. Евсеев С.П. Анализ програмной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования / С.П. Евсеев, Х.Н. Рзаев, А.С. Цыганенко // Безпека інформації 2016. – Том 22, № 2. – Киев: Наш формат, 2016. – С. 196-203.

6. Евсеев С.П. Математическая модель протокола обмена данными на основе модифицированных несимметричных крипто-кодовых систем Мак-Элиса и Нидеррайтера на ущербных кодах / С.П. Евсеев, О.Г. Король // Захист інформації і безпека інформаційних систем: матеріали VI Міжнар. наук.-техн. конф. – Львів: Видавництво Львівської політехніки, 2017. – С. 89-90.

7. Грищук Р.В. Основи кібербезпеки / Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

8. Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. – М.: Мир, 1986.

9. Rukhin A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto // NIST Special Publication 800-22, 2000.

10. Biswas Bhaskar. McEliece Cryptosystem Implementation: Theory and Practice. – 2008. – P. 47-62.

11. Manna Sarbajit. Design and implementation of a two-layered hybrid cryptosystem / Manna Sarbajit, Prajapati Mohit, Sett Ayan, Banerjee Kallol, Dutta Saurabh. – 2017. – P. 327-331.

12. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theory. – 1986. – V.15. – P. 19-34.

13. Hee Cheon Jung. A Practical Post-Quantum Public-Key Cryptosystem Based on $$textsf {spLWE}$$ / Hee Cheon Jung, Kyoohyung Han, Kim Jinsu, Lee Changmin, Son Yongha. // Lecture Notes in Computer Science. – 2017. – Vol. 10157. – P. 51-74.

14. Berlekamp E.R. Factoring Polynomials Over Large Finite Fields / E.R. Berlekamp // Bell System Technical Journal. – 1967.

15. Report on Post-Quantum Cryptography [Електронний ресурс]. – Режим доступу до ресурсу: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

16. Sendrier Nicolas. The tightness of security reductions in code-based cryptography / Sendrier Nicolas // 2011 IEEE Information Theory Workshop, ITW 2011. – 2011. – P. 415-419.

17. Security requirements for cryptographic modules [Електронний ресурс]. – Режим доступу до ресурсу: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. (Accessed on December 1, 2017).

18. Іванченко І.С. Забезпечення інформаційної безпеки держави / І.С. Іванченко, В.О. Хорошко, Ю.Е. Хохлачова, Д.В. Чирков; за заг. ред. проф. В.О. Хорошка. – К: ПВП "Задруга", 2013. – 170 с.

References

1. Bolotov, A.A. (2000), "*Algorytmycheskye osnovy ellyptycheskoj kryptografyy*" [*Algorithmic foundations of elliptical cryptography*], MEY, Moscow.

2. Myshhenko, V.A. and Vylanskyj, Ju.V. (2007), "*Ushherbnye teksty y mnogokanal'naja kryptografyja*" [*Distorted texts and multichannel cryptography*], Encyklopedyks, Mynsk.

3. Sydel'nykov, V.M. (2002), "Kryptografyja y teoryja kodyrovanyja" [Cryptography and coding theory], *Materyaly konferencyy "Moskovskyj unyversytet y razvytye kryptografyy v Rossyy"*, MGU, Moscow, pp. 1-22.

4. Gryshhuk, R.V. and Danyk, Ju.G. (2016), "*Osnovy kibernetychnoi' bezpeky: monografija*" [*Fundamentals of cybernetic security: monograph*], ZhNAEU, Zhytomyr.

5. Evseev, S.P., Rzaev, H.N. and Cyganenko, A.S. (2016), "Analyz programnoj realyzacyy prjamogo y obratnogo preobrazovanyja po metodu nedvoychnogo ravnovesnogo kodyrovanyja" [Analysis of the software implementation of direct and inverse transformation using the non-binary equilibrium coding method], *Bezpeka informacii'*, Vol. 22, No. 2, Kyiv, pp.196-203.

6. Evseev, S. P. and Korol', O.G. (2017), "Matematycheskaja model' protokola obmena dannymy na osnove modyfycyrovannyh nesymmetrychnyh krypto-kodovyh system Mak-Elysa y Nyderrajtera na ushherbnyh kodah" [Mathematical model of the protocol of data exchange on the basis of modified asymmetric crypto-code systems of McElice and Niederraiter on flawed codes], *Zahyst informacii' i bezpeka informacijnyh system*, Vydavnyctvo L'vivs'koi' politehniky, L'viv, pp. 89-90.

7. Gryshhuk R.V. and Danyk, Ju.G. (2016), "*Osnovy kiberbezpeky*" [*Cybersecurity Basics*], ZhNAEU, Zhytomyr, 636 p.

8. Blejhut, R. (1986), "*Teoryja y praktyka kodov, kontrolyrujushhyh oshybky*" [*Theory and practice of error control codes*], Myr, Moscow.

9. Rukhin, A. and Soto, J. (2000), A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, *NIST Special Publication, 800-22*.

10. Biswas, Bhaskar and Sendrier, Nicolas (2008), *McEliece Cryptosystem Implementation: Theory and Practice*, pp. 47-62.

11. Manna, Sarbajit, Prajapati, Mohit, Sett, Ayan, Banerjee, Kallol and Dutta, Saurabh (2017), *Design and implementation of a two-layered hybrid cryptosystem*, pp. 327-331.

12. Niederreiter, H. (1986), Knapsack-Type Cryptosystems and Algebraic Coding Theory, *Probl. Control and Inform. Theory*, Vol. 15, pp. 19-34.

13. Hee Cheon, Jung, Kyoohyung, Han, Kim, Jinsu, Lee, Changmin and Son, Yongha (2017), A Practical Post-Quantum Public-Key Cryptosystem Based on $$textsf {spLWE}$$, *Lecture Notes in Computer Science*, Vol. 10157, pp. 51-74.

14. Berlekamp, E.R. (1967), Factoring Polynomials Over Large Finite Fields, *Bell System Technical Journal*.

15. *Report on Post-Quantum Cryptography*, www.nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

16. Sendrier, Nicolas (2011), The tightness of security reductions in code-based cryptography, *IEEE Information Theory Workshop ITW 2011*, pp. 415-419.

17. *Security requirements for cryptographic modules*, https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, Accessed on December 1, 2017.

18. Ivanchenko, I.S., Horoshko, V.O., Hohlachova, Ju. E. and Chyrkov, D.V. (2013), "*Zabezpechennja informacijnoi' bezpeky derzhavy*" [*Providing information security of the state*], Zadruga, Kyiv, 170 p.

Надійшла до редколегії 18.05.2018
Схвалена до друку 19.06.2018

Інформація про авторів:

Євсєєв Сергій Петрович
кандидат технічних наук старший науковий співробітник
доцент кафедри Харківського національного
економічного університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0003-1647-6444

Циганенко Олексій Сергійович
аспірант Харківського національного
економічного університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0002-5784-8438

Information about the authors:

Serhii Yevseiev
PhD, Senior Research
Senior Lecturer of Department of
Simon Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0003-1647-6444

Oleksii Tsyhanenko
Postgraduate Student of Simon Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-5784-8438

РАЗРАБОТКА НЕСИММЕТРИЧНОЙ КРИПТО-КОДОВОЙ КОНСТРУКЦИИ НИДЕРРАЙТЕРА НА МОДИФИЦИРОВАННЫХ КОДАХ

С.П. Евсеев, А.С. Цыганенко

Рассматривается способы модификации линейных блочных кодов (эллиптических кодов) для построения крипто-кодовых конструкций. Подробно рассмотрен метод модификации путем укорочения. Рассмотрена математическая модель модифицированной несимметричной крипто-кодовой системы (МНККС) Нидеррайтера на эллиптических кодах. Предлагаются прикладные алгоритмы формирования и расшифровки криптограммы в МНККС на основе модифицированных крипто-кодовых конструкций. Разработана блок-схема алгоритмов формирования и расшифровки криптограммы в МНККС Нидеррайтера на основе модифицированных крипто-кодовых конструкций с учетом особенностей реализации. Проведено исследование свойств модифицированной НККС Нидеррайтера: исследована зависимость сложности формирования криптограммы, сложности декодирования криптограммы, сложности взлома и сложности кодирования. По результатам исследований, несмотря на уменьшение мощности поля для МНККС, характеристики таких крипто-кодовых конструкций оказались, как минимум, не хуже традиционной НККС Нидеррайтера. Таким, образом рассмотрена МНККС Нидеррайтера является конкурентоспособной системой обеспечения основных услуг безопасности и перспективным направлением исследований по снижению энергозатрат крипто-преобразований в ККС с использованием кодовых конструкций, путем их модификации.

Ключевые слова: *несимметричные крипто-кодовые системы, модифицированные крипто-кодовые конструкции, укороченные коды, Нидеррайтер.*

DEVELOPMENT OF ASYMMETRICAL CRYPTO-CODED CONSTRUCTION OF NIDERRAITER ON MODIFIED CODES

S. Yevseiev, O. Tsyhanenko

Methods of modifying linear block codes (elliptic codes) for constructing crypto-code designs are considered. The modification method is shortened in detail. The mathematical model of the modified asymmetric crypto-code system (MACCS) of the Nethereright on elliptic codes is considered. Applied algorithms for the formation and decryption of cryptograms in MACCS on the basis of modified crypto-code designs are offered. A block diagram of algorithms for the formation and decryption of cryptograms in the ACCS Niderraiter based on modified crypto-code designs, taking into account the peculiarities of implementation, has been developed. The research of the properties of the modified ACCS Niderraiter was carried out: the dependence of the complexity of the formation of cryptograms, the complexity of decrypting the cryptogram, the complexity of the burglary and the complexity of coding have been investigated. According to the results of the research, despite the reduction of field strength for the MACCS, the characteristics of such crypto-code designs were, at least, not worse than the traditional ACCS Niderraiter. In this way, the MACCS of Niderraiter is a competitive system for providing basic security services and is a promising direction of research on reducing energy consumption of cryptographic transformations in CCS using code structures, by modifying them.

Keywords*: asymmetrical crypto-code systems, modified crypto-code constructions, shortened codes, Niderraiter.*