КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1061
УДК 681.32:007.5

Дунаєв Сергій Владиславович
аспірант кафедри кібербезпеки
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна
ORCID: 0000-0001-8736-3602
serg.dynaev@gmail.com

РОЗРОБКА КРИПТО-КОДОВИХ КОНСТРУКЦІЙ НА ОСНОВІ АЛГЕБРАЇЧНИХ ТА LDPC, ЗБИТКОВИХ КОДАХ

Анотація. Розвиток постквантових технологій становить під сумнів криптостійкість сучасних симетричних та несиметричних криптосистем. З появою повномасштабного квантового комп'ютера такі системи не зможуть забезпечувати необхідний рівень криптостійкості (рівень 5 за шкалою спеціалістів НІСТ США). Проведений конкурс на постквантові алгоритми виявив тенденцію побудови криптосистем на основі синтезу (комплексуванню) теорій захисту з теорією Галуа. Серед переможців постквантових алгоритмів окремо виділені крипто-кодові конструкції (ССС) Мак-Еліса та Нідеррайтера, які дозволяють інтегровано забезпечити необхідний рівень захисту та інтегровано підвищити рівень вірогідності передачі інформації. Але суттєвим недоліком є можливість зламу таких систем на лінійних кодах, а також необхідність їх побудови на полем Галуа 2^{10}–2^{13}, що значно зменшує їх можливість щодо побудови систем на основі смарт-технологій та mesh-мереж. В роботі пропонується використання симетричної ССС (SCCC) на основі схеми Рао-Нама (SCCC R-N) на алгеброгеометричних (ЕС – еліптичні коди, МЕС – модифіковані еліптичні коди), LDPC та збиткових кодах, що забезпечує можливість забезпечить значного зменшення об'єму ключових даних (побудова ККК над полем на Галуа 2^4–2^6) при зберіганні рівня стійкості та вірогідності передачі інформації (безпечний час 10^{25}–10^{35}). Такий підхід забезпечує можливість формування інтелектуальних систем захисту інформації (ІСЗІ). Метою дослідження є розробка постквантових алгоритмів на основі комплексування теорій побудови криптосистем симетричної та несиметричної криптографії з методами побудови завадостійких кодів. Такий підхід дозволяє забезпечити регулювання необхідного рівня стійкості криптосистеми на основі вимог щодо секретності інформаційного повідомлення, а також його часу зберігання рівня стійкості системи в цілому.

Ключові слова: крипто-кодові конструкції Рао-Нама, алгебраїчні коди, LDPC та збиткові коди.

ВСТУП

Розвиток обчислювальних можливостей повномасштабного квантового комп'ютера , поява нових сфер використання штучного інтелекту, синтез смарт-технологій з Інтернет речами формує нові більш жорсткі вимоги щодо побудови систем захисту інформації. Найбільш використовуються алгоритми симетричної криптографії (довжина ключа 128-256 біт) можуть бути зламані на основі квантового алгоритму Гровера. Криптосистеми на основі криптографії з відкритим ключем, включаючи і криптографію на еліптичних кривих, повномасштабний квантовий комп'ютер може вирішити (зламати), використовуючи алгоритм Шора [1; 2; 3]. Майже вся асиметрична криптографія, яка використовується сьогодні, може бути ефективно зламана квантовими алгоритмами [4,5]. В умовах можливого криптографічного «хаосу», який пов'язаний з появою повномасштабного комп'ютера спеціалістами НІСТ США був проведений конкурс на постквантові алгоритми, у якому приймали участь крипто-кодові конструкції

Мак-Еліса на кодах Гопи [6–11]. Сутність крипто-кодових конструкцій полягає у комплексуванні методів завадостійкого кодування з методами побудови несиметричних алгоритмів. Криптостійкість таких систем базується на теоретико-складної задачі – декодування випадкового коду. Для цього у ССС використовуються матриці маскування, які складають особистий (закритий) ключ для кожного користувача системи, а потім на основі їх перемноження з породжувальною матрицею циклічного завадостійкого коду формується відкритий (публічний) ключ користувача [12–14]. Відомі ССС, які формують несиметричні криптосистеми це схеми Мак-Еліса, Нідеррайтера [8–9], а також крипто-кодова конструкція Рао-Нама яка будує симетричну криптосистему [10–11]. Крім забезпечення відповідних рівнів криптостійкості крипто-кодові конструкції, які будують несиметричні криптосистеми за швидкістю порівняні з симетричними блоковими шифрами, а також завадостійке кодування додає інтегрований механізм – боротьбу з помилками у каналі передачі. Таким чином, використання інтегрованих механізмів забезпечення необхідного рівня послуг безпеки та вірогідності при передачі даних є актуальним завданням.

Постановка проблеми. Квантові комп'ютери вже успішно розкладають малі цілі числа [10–11]. Таким чином, зловмисник може зберігати перехоплені обміни ключами та зашифровані тексти сьогодні та дешифрувати їх, коли буде доступний великомасштабний квантовий комп'ютер. Залежно від того, коли (і якщо) стануть доступними потужні квантові комп'ютери, це може зробити симетричну та асиметричну криптографію «непридатною» для шифрування ключових даних і передачі конфіденційної інформації. Проведений конкурс на постквантові алгоритми показав необхідність комплексування сучасних теорій побудови спеціальних механізмів криптографічного захисту, що підтверджується архітектурним рішенням переможців конкурсу НІСТ США. Однак використання переможців на основі теорії ґраток не завжди можливо за рахунок їх обчислювальних потреб. Тому перспективним напрямом є розробка постквантових алгоритмів з меншими потребами не тільки в обчислювальних, а також енергоємних вимогах, при забезпеченні необхідного рівня безпеки.

Аналіз останніх досліджень і публікацій. Дослідження проблеми виявлення сигналів засобів негласного отримання Проведений аналіз в [12,13] показав, що стійкість ССС Мак-Еліса базується на NP-повної задачі – декодування випадкового лінійного коду. Основна ідея, яка використовується в таких системах базується на використанні матриць маскування. Швидкість кодування (криптоперетворень) значно вище ніж у криптосистем з відкритим ключем, але об'єм ключових даних значно вище. Таким чином, з одного боку (перше) є перевагою, з іншого (друге) – суттєвим недоліком. В роботах [14–15] наведені результати досліджень криптостійкості ССС з відкритим ключем, показаний дієвий алгоритм зламу несиметричних криптосистем Мак-Еліса на кодах Ріда-Соломона. За рахунок ортогональності матриць (породжувальна G та перевірочна H, $\|G\|\times\|H\|T=\|0\|$) алгоритм може бути застосований також к ССС Нідеррайтера, запропоноване використання алгеброгеометричних кодів (коди, які будуються на еліптичних кривих) або каскадних кодів. В роботі [16] запропоновані ССС Мак-Еліса на квазіциклічних кодах перевірки парності з низькою щільністю, які дозволяють подолати основні обмеження оригінальної криптосистеми. Це дозволяє забезпечити протидію атаки Сідельнікова, але збільшують об'єм ключових даних. В роботі [17] запропонована симетрична криптосистема на схемі Рао-Нама з гіперхаотичною системою дробового порядку та розширеній квазіциклічній перевірці парності з низькою щільністю (EDF–QC–LDPC)-кодів. Запропонована чотиривимірна гіперхаотична система дробового порядку, яка забезпечує формування псевдовипадкової

послідовності. Завдяки заміні синдромів помилок псевдовипадковою послідовністю та динамічній перестановці кодованого повідомлення забезпечується стійкість, але при цьому збільшується об'єм ключових послідовностей. Таким чином, проведений аналіз використання ССС Мак-Еліса та Нідеррайтера показав, що таки системи забезпечують побудову несиметричних криптосистем та інтегровано забезпечують підвищення рівня вірогідності отримання інформації. Але використання завадостійких кодів на забезпечує у повному обсязі необхідний рівень стійкості у постквантовий період та потребує використання алгеброгеометричних кодів. Крім цього залишається значний обсяг ключових даних, що обмежує їх практичне використання в смарт- та мобільних технологіях. SCCC R-N дозволяє «зняти» ці недоліки але їх побудова на класичних циклічних кодах не забезпечує необхідну стійкість до атак у квантовий період.

Метою даної статті є розробка постквантових алгоритмів на основі комплексування теорій побудови криптосистем симетричної та несиметричної криптографії з методами побудови завадостійких кодів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

З метою побудови стійкої до атаки Сідельнікова – знаходження елементів породжувальної матриці за рахунок операцій на гомоморфізмами (злам особистого ключа) пропонується використовувати алгеброгеометричні коди – поєднання завадостійкого кодування з геометричними параметрами еліптичних кривих [20].

Такий підхід забезпечує додатку ентропію, що додає необхідний рівень криптостійкості, а також забезпечує протидію вказаної атаки.

Для забезпечення криптостійкості у SCCC R-N використовується матриця маскування – породжувальна матриця G. Для забезпечення додаткової ентропії – використовується вектор помилки, який формує сеансовий ключ кожного повідомлення (криптограми). Криптограма (кодограма) формується на основі виразу [10–11,21]:

$$c = IG^T + e, \tag{1}$$

де $I = \{I_1, I_2, \ldots, I_k\}$ – інформаційний вектор, $e = \{e_1, e_2, \ldots, e_n\}$ – випадковий вектор помилок, ваги $w(e) \leq t$, де t – виправляюча здатність завадостійкого коду [21].

У модифікованій SCCC R-N (SMCCC R-N) для забезпечення додаткового рівня стійкості використовується додаткова матриця маскування Z. Матриця маскування Z розміром $n \times n$, є матрицею переставлення (у кожному стовпці та рядку по одиниці) [20–28]. Криптограма формується за виразом [21]:

$$c = (IG^T + e) \times Z, \tag{2}$$

Для побудови алгеброгеометричних кодів на основі еліптичних кривих використовуються алгоритми які запропоновані у [20–28]. Такий підхід забезпечує формування породжувальної матриці на основі використання проекцій точок еліптичної кривої $P_i(X_i, Y_i, Z_i)$ в генераторних функцій. Значення генераторних функцій від визначених точок забезпечує формування породжувальної матриці еліптичного коду [20–28], яка визначена виразом:

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j\left(P_i\right) \right\|_{n,k}, \quad (3)$$

В афінному просторі A^2 над полем $GF(q)$ еліптична крива задається виразом [20–28]:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, \quad (4)$$

у проєктивному просторі P^2 [16–19]:

$$y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3, \quad (5)$$

де $a_i \in GF(q)$, род кривої $g=1$.

Загальна кількість точок кривої визначається виразом Хасе-Веля [16–19]:

$$N \le 2\sqrt{q} \cdot g + q + 1, \quad (6)$$

де g – род кривої, $q = p^m$ поля Галуа.

Таким чином, межа Хасе-Веля визначає максимальну кількість точок, які можуть бути визначені у якості елементів еліптичного коду. Алгеброгеометричний (n, k, d)-код задає наступні параметри завадостійкого коду: $k+d \ge n$, $n \le 2\sqrt{q}+q+1$, $k \ge \alpha$, $d \ge n-\alpha$, $\alpha = 3 \times degF$ [20–28]. Для забезпечення криптостійкості спеціалісти НІСТ США рекомендують будувати ССС з використанням завадостійких кодів з елементами на GF (2^{10}–2^{13}), що дуже складно реалізувати в mesh-мережах на основі смарт-технологій та технологій бездротового зв'язку [1,2,21]. Таким чином, необхідний підхід щодо скорочення множини поля Галуа зі збереженням рівня криптостійкості системи у цілому. Зниження ємності та обчислювальної складності побудови ССС можливо на основі МЕС, побудова яких запропонована в [20–28]. При цьому для забезпечення необхідного рівня стійкості серед параметрів завадостійкого коду необхідно зафіксувати параметр d – конструктивна відстань, яка визначає кількість визначення та виправлення помилок у кодовому слові [20–28].Таким чином, для забезпечення необхідного рівня стійкості SCCC R-N необхідно використовувати способи модифікації, що не допускають зниження мінімального кодової відстані [20–28]. Проведений аналіз способів модифікації параметрів циклічних кодів показав, що d (конструктивна відстань) не змінюється при використанні параметрів завадостійкого коду при їх скорочені (скорочується кількість символів у кодовому слові).

Сутність методу модифікації – скорочення полягає у видалені визначених вектором ініціалізації (IV_1) символів кодового слову, при цьому враховується конструктивна кодова відстань, яка забезпечує відповідну кількість виявлення та виправлення помилок [20–28]. Вектор ініціалізації (IV_1) забезпечує компенсацію рівня стійкості при зменшені потужності поля. Такий підхід забезпечує формування модифікованих еліптичних кодів (МЕС). Сутність методу модифікації завадостійкого коду – подовження – полягає в додаванні, після скорочення кодового слову, символів відкритого тексту на основі другого вектору ініціалізації (IV_2), який визначає місця додавання, при цьому

враховується довжина кодового слова. Звичайно другий вектор ініціалізації (IV_2), також підвищує рівень криптостійкості SCCC R-N [21].

Для подальшого зменшення енергетичних та обчислювальних витрат на програмну (програмно-апаратну реалізацію) зі збереженням рівня стійкості пропонується гібридна ККК (HCCC) R-N з *MEC* на основі використання збиткових кодів (DC). Формування HCCC базується на зменшені збитковості кожного символу (визначається будь-яким протоколом сигнально-кодових конструкцій, наприклад ASCII-таблиця) [27–28]. При цьому використовується алгоритм скорочення MV2 забезпечує сюрективне відображення елементів коду та визначає збиток, який формує генератор псевдовипадкових чисел (ГПВЧ) та збитковий текст (сформований після нанесення збитку) [29–30]. Такий підхід формує багатоканальну криптографію за рахунок передачі двома відкритими каналами зв'язку передачу збитку та збиткового коду, основні теоретичні основи збиткових кодів та параметрів CCC на FC наведені у [27–30].

Таким чином, симетрична крипто-кодова конструкція Рао-Нама при використанні EC (MEC), збиткових кодах забезпечує необхідний рівень безпеки, та можливість використання у системах на основі смарт-технологій та mesh-мереж.

Для забезпечення безпеки елементів інфраструктури ОКІ в умовах постквантового періоду (появи повномасштабного комп'ютера) пропонується використовувати SCCC R-N на еліптичних кодах (EC), модифікованих (скорочених та/або подовжених) EC (MEC), кодах LDPC, а також збиткових кодах. такий підхід не тільки забезпечує різні рівні безпеки (відповідно вимогам конкурсу на постквантові криптоалгоритми NIST),а також забезпечує можливість створення SCCC/HCCC R-N, які відповідають вимогам стійкості у постквантовий період.

Для побудови SCCC R-N на LDPC-кодах розглянемо опис алгоритму кодування/разкодування. Коди з низькою щільністю перевірок на парність (Low-Density Parity-Check, LDPC) є класом лінійних блокових кодів, що володіють високою коригуючою здатністю та наближаються до теоретичної межі Шеннона. Наданий програмний код, реалізований на мові Python з використанням бібліотеки pyldpc, моделює повний цикл передачі даних через зашумлений канал із застосуванням LDPC-коду. Цей аналіз систематизує та деталізує кожен етап алгоритму відповідно до наданої блок-схеми, розкриваючи математичні та логічні основи операцій.

Етап 1: Кодування

Цей етап включає ініціалізацію параметрів, створення структури коду, генерацію інформаційного повідомлення та його перетворення у кодове слово, захищене від помилок.

1.1. Ініціалізація параметрів та побудова коду

На початковому етапі відбувається ініціалізація ключових параметрів LDPC-коду:

- $n\_code = 30$: Довжина кодового слова (n), тобто загальна кількість бітів після кодування.
- $d\_v = 3$: Ступінь вузлів змінних (кількість одиниць у кожному стовпці перевірочної матриці **H**).
- $d\_c = 5$: Ступінь перевірочних вузлів (кількість одиниць у кожному рядку матриці **H**).

Далі, за допомогою функції

$$make\_ldpc(n, d\_v, d\_c, systematic = True, sparse = True)$$

генеруються дві фундаментальні матриці:

1. **Перевірочна матриця H (Parity-Check Matrix)**: Розріджена матриця, яка визначає кодові обмеження. Будь-яке кодове слово **c** повинно задовольняти умову $cdotc^T = 0$.
2. **Породжуюча матриця G (Generator Matrix)**: Використовується для кодування інформаційного повідомлення. Параметр systematic=True забезпечує побудову матриці **G** у систематичній формі $[I_k \mid P]$, де I_k — одинична матриця розмірності k (довжина інформаційного повідомлення), а **P** — матриця парності. Це значно спрощує процес вилучення вихідного повідомлення після декодування.

1.2. Генерація та кодування повідомлення

Після створення матриць визначається розмір інформаційного повідомлення $k = G.shape[1]$. Генерується випадковий двійковий вектор input_message довжиною k.

Процес кодування полягає у виконанні матрично-векторного добутку в полі Галуа $GF(2)$:

$$d = utils.binaryproduct(G, input\_message)$$

В результаті отримуємо кодове слово **d** (вектор довжиною n), яке є лінійною комбінацією рядків матриці **G** з коефіцієнтами з input_message.

1.3. Модуляція сигналу

Для симуляції передачі через аналоговий канал, двійкове кодове слово d піддається двійковій фазовій маніпуляції (BPSK - Binary Phase-Shift Keying). Біти $\{0, 1\}$ відображаються у фізичні рівні сигналу $\{+1, -1\}$:

$$encoded\_message = (-1) ** d$$

Цей крок є стандартним для підготовки сигналу до передачі через канал з адитивним білим гаусовим шумом (AWGN).

Етап 2: Канал з шумом

На цьому етапі симулюється проходження модульованого сигналу через канал зв'язку, де виникають помилки. У даній реалізації використовується детермінована модель каналу, яка вносить фіксовану кількість помилок (error_count = 2).

Процес симуляції помилок реалізовано циклічно:

1. Вибирається випадкова позиція error_pos у векторі encoded_message.
2. Значення сигналу в цій позиції інвертується ($error\_message[error\_pos] = -1 * error\_message[error\_pos]$),
   що еквівалентно бітовій помилці ($0 \rightarrow 1$ або $1 \rightarrow 0$).

В результаті отримуємо вектор error_message, який є зашумленою версією переданого кодового слова.

Етап 3: Декодування та Аналіз

Це фінальний етап, на якому відбувається спроба відновити вихідне інформаційне повідомлення з зашумленого сигналу.

3.1. Процес декодування

Центральною операцією є виклик функції $decode(H, error\_message, snr, maxiter = 100)$. Ця функція реалізує ітеративний алгоритм декодування, такий як алгоритм поширення переконань (Belief Propagation).

- **Вхідні дані:**
  - H: Перевірочна матриця, що задає структуру коду.
  - error_message: Отриманий зашумлений сигнал.

- snr: Співвідношення сигнал/шум (Signal-to-Noise Ratio), що характеризує якість каналу.
- maxiter: Максимальна кількість ітерацій алгоритму.

- **Процес:** Алгоритм ітеративно обмінюється повідомленнями між вузлами змінних та перевірочними вузлами графа Теннера, що відповідає матриці **H**, намагаючись знайти найбільш ймовірне кодове слово, яке задовольняє всім перевіркам на парність.
- **Вихід:** decoded_message — відновлене кодове слово у двійковому форматі.

3.2. Вилучення повідомлення та аналіз результату

Завдяки використанню систематичного коду, вилучення вихідної інформації є тривіальним. Функція $get\_message(G, decoded\_message)$ просто повертає перші k біт з відновленого кодового слова decoded_message.

Останній крок — верифікація результату. Кількість помилок у відновленому повідомленні обчислюється як сума модулів різниць між вихідним та відновленим повідомленнями:

$$errors = abs(restored\_message - input\_message).sum()$$

Нульове значення errors свідчить про успішне та повне відновлення вихідних даних, демонструючи ефективність LDPC-коду.

Таким чином, наведений програмний код є комплексною симуляцією, що наочно ілюструє всі ключові етапи функціонування системи зв'язку на основі LDPC-кодів. Алгоритм послідовно реалізує побудову коду, кодування інформації, імітацію канальних спотворень та потужний ітеративний процес декодування. Результати симуляції підтверджують високу коригуючу здатність кодів з низькою щільністю перевірок на парність, що обґрунтовує їх широке застосування в сучасних системах передачі даних.

Симетрична криптосистема на основі крипто-кодової конструкції Рао-Нама на EC будується за правилом [10,11,21]:

$$c^* = i \times G^{EC} + e, \tag{7}$$

де G^{EC} – породжувальна матриця еліптичного коду розмірністю $k \times n$ над $GF(q)$ – секретний ключ криптосистеми, i – k-розрядний інформаційний вектор, вектор e – секретний вектор помилок вагою $\leq t$ (виправляюча здатність коду).

Схему протоколу SCCC R-N з використанням EC наведено рис. 1 [10,11,21].

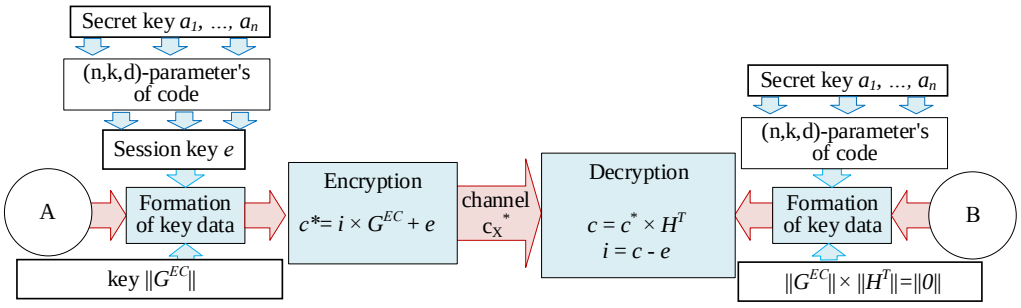

Рис.1. Схема протоколу передачі даних на основі SCCC R-N з EC

Симетрична криптосистема на основі SMCCC на EC формується за правилом [10,11,21]:

$$c^* = \left(i \times G^{EC} + e\right) \times Z, \tag{8}$$

де G^{EC} – породжувальна матриця EC розмірністю $k \times n$ над $GF(q)$, Z – переставна матриця (у кожному стовбці та строки одна одиниця) розмірністю $n \times n$ – матриця маскування.

Схему протоколу SMCCC R-N з використанням ЕС наведено рис. 1 [21].

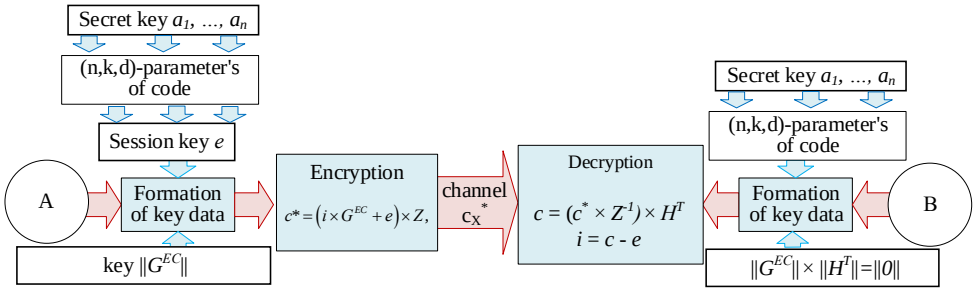

Рис. 2. Схема протоколу передачі даних на основі SMCCC R-N з ЕС

SCCC R-N (n, k, d)-код над $GF(q)$ задає наступні параметри: $k+d \geq n$, $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \times degF$. Складність алгоритму несистематичного кодування формально складає $O(3 \times degF \times n)$ або $O((n-d) \times n)$.

Для побудови SCCC R-N на МЕС над $GF(2^6–2^8)$ використовуються методи скорочення та подовження кодового слова, які забезпечують необхідний рівень безпеки симетричної криптосистеми, а також швидкість криптоперетворення та зниження обчислювальної складності реалізації [21].

На рис. 3, 4 наведені протоколи обміну на основі SCCC R-N на *МЕС* (скорочених, подовжених), на рис. 5, 6 – на основі SMCCC R-N на *МЕС* (скорочених, подовжених) [21].

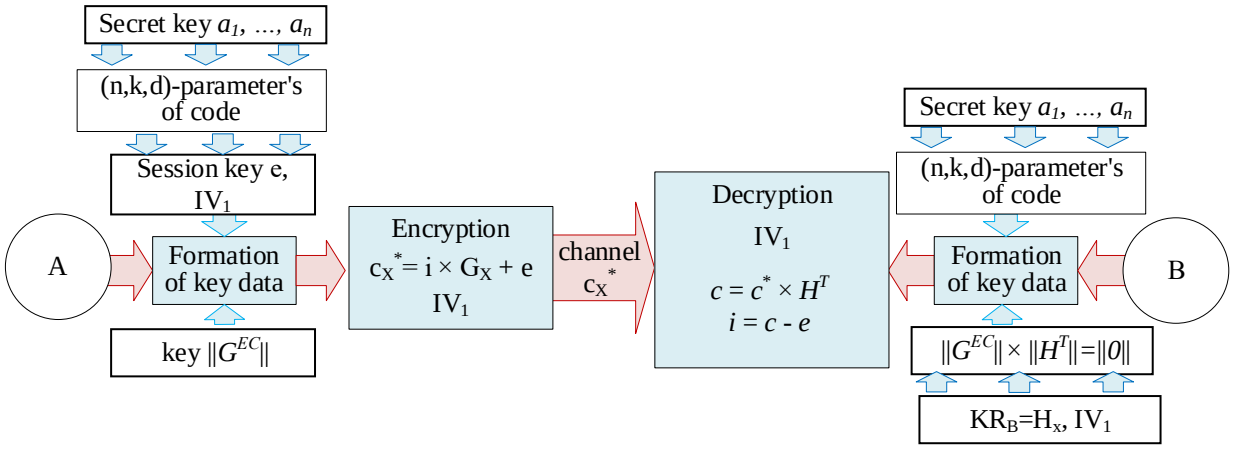

Рис. 3. Схема протоколу передачі даних на основі SCCC R-N з МЕС (скорочені коди)

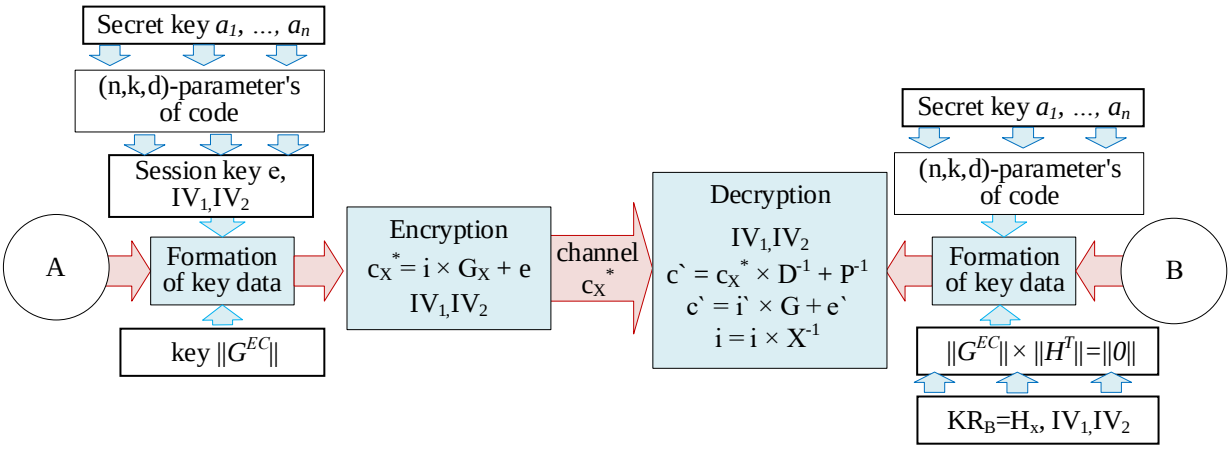

Рис. 4. Схема протоколу передачі даних на основі SCCC R-N з MEC (подовжені коди)

Основні властивості *MEC* та параметри постквантових криптосистем на основі схем SCCC R-N на *MEC* наведені у [20–28].

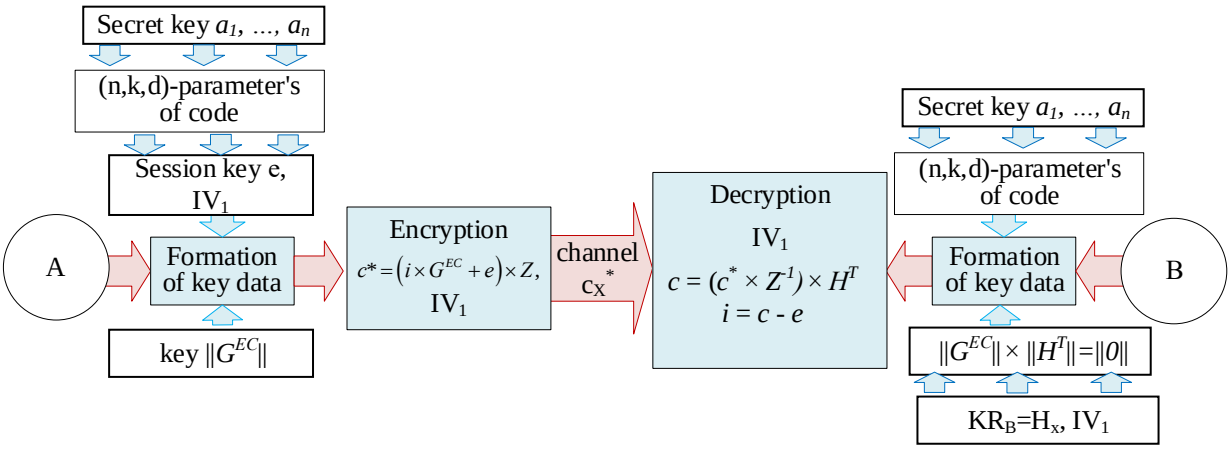

Рис. 5. Схема протоколу передачі даних на основі SMCCC R-N з MEC (скорочені коди)

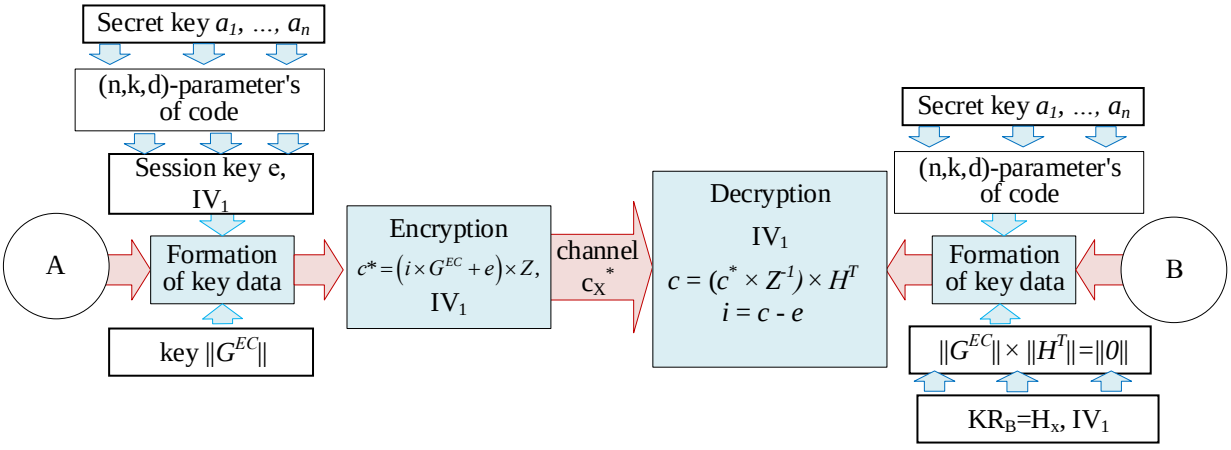

Рис. 6. Схема протоколу передачі даних на основі SMCCC R-N з MEC (подовжені коди)

Запропоновані рішення побудови симетричної криптосистеми на основі SCCC R-N забезпечує 5 рівень стійкості за шкалою НІСТ США, а також можливість використання в сучасних протоколах цілісності SSL/TLS. Для побудови HCCC R-N над полями Галуа (2^4–2^6) використовується алгоритм MV2 багатоканальної криптографії – основу якої складають збиткові коди [26–27]. В [26–27] запропоновані схеми використання багатоканальної криптографії на основі збиткових кодів. При цьому підхід 1 забезпечує нанесення збитку початковому тексту з подальшим шифруванням збиткового тексту і / або його збитків; підхід 2: нанесення збитку шифртексту; підхід 3: нанесення збитку вихідному тексту і шифртексту збиткового тексту. Для нанесення збитку використовується ПВП (збиток), яка визначає яку кількість бітів видаляється з ASSCII-послідовності символу відкритого тексту. Після чого остаток символів формують збитковий текст.

Проведений аналіз використання алгоритму MV2 (алгоритму нанесення збитку) показав, що кращий результат забезпечується при виконанні наступних послідовностей – з початку шифрування у SCCC R-N, потім нанесення збитку до шифртексту (підхід 3). На рис. 7, 8 наведені схеми побудови гібридної SCCC R-N /SMCCC R-N на скорочених еліптичних кодах [26–27].

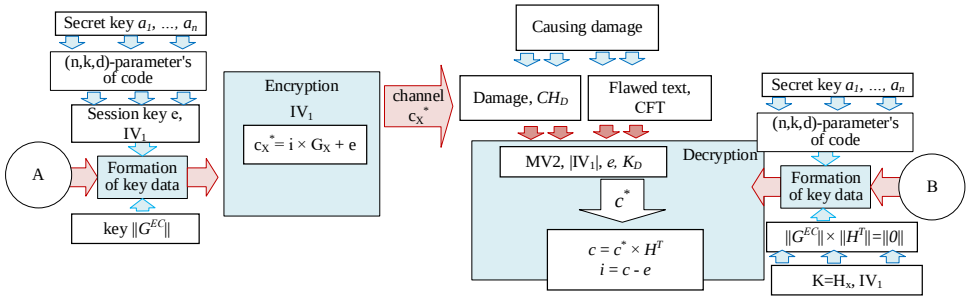

Рис. 7. Схема протоколу передачі даних на основі HCCC R-N з МЕС (скорочені коди)

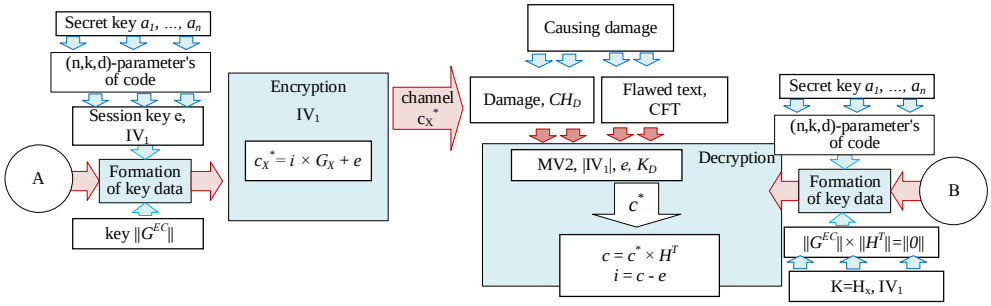

Рис. 8. Схема протоколу передачі даних на основі HCCC R-N з МЕС (скорочені коди)

Запропонований підхід забезпечує необхідний рівень стійкості (за рахунок багатоканальної криптографії на збиткових кодах), вірогідності, та значно зменшує об’єм ключових даних. Крім цього, для зменшення ключових даних та підвищення рівня захищеності ключових даних можливий обмін тільки коефіцієнтами рівняння еліптичної кривої між учасниками протоколу. Такий підхід забезпечує передачу не всього кортежу векторів ключових даних, що також зменшує загальний об’єм ключової інформації [26–27].

Для проведення досліджень запропонована SCCC R-N на алгеброгеометричних кодах програмно реалізована мовою C++. Програмно-апаратна реалізація ККК реалізована на Raspberry Pi3, модель B+ (RPI3-MODBP) яка базується на SoC (система-на-чипі) BCM2837B0. Результати порівняльних досліджень SCCC R-N наведені на рис. 9, 10 [21].

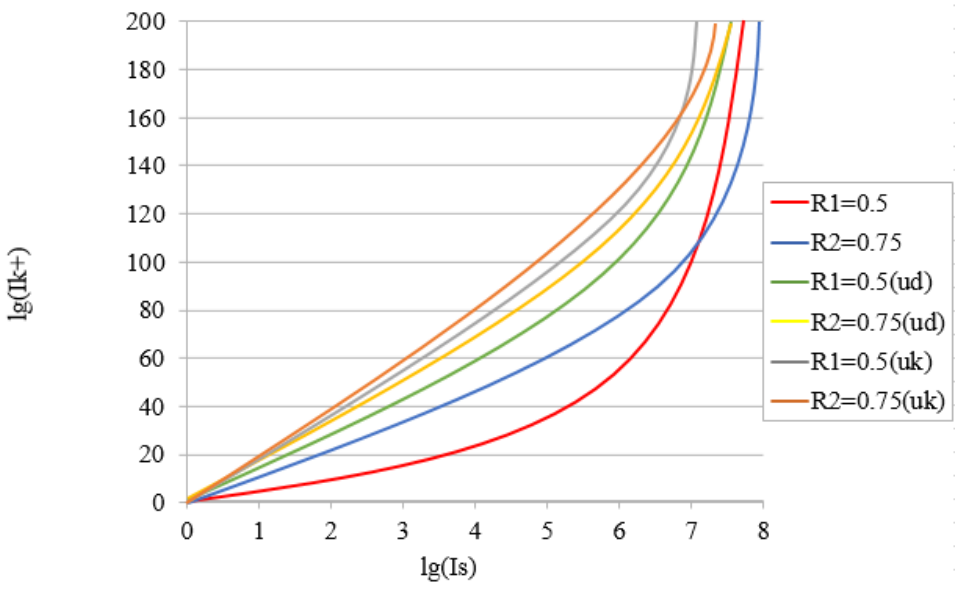

Рис.9. Зведена діаграма складності злому і складності кодування SCCC R-N на МЕС (скорочених та подовжених кодах)

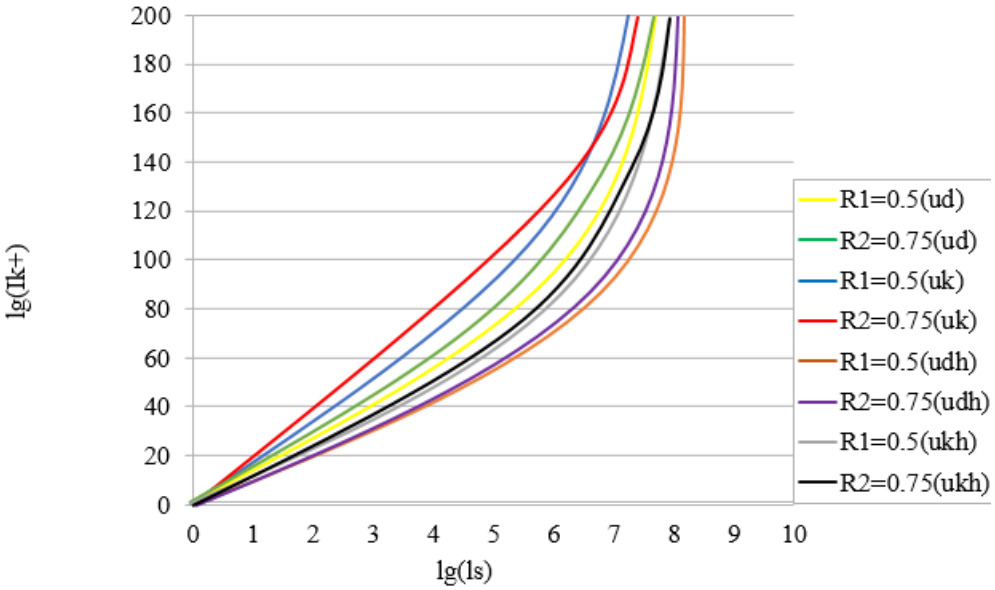

Рис.10. Зведена діаграма складності злому і складності кодування HCCC R-N

Аналіз рис. 9, 10 показав, що використання HCCC R-N значно зменшує обчислювальну складність кодування/шифрування (біля 12, 5 разів у порівнянні з CCC на EC), та разкодування (біля 20 разів), при цьому забезпечується необхідний рівень безпеки [21].

Для підтвердження рівня стійкості використаний розроблений експертами НІСТ США у 2000 році пакет NIST STS 822, який забезпечує перевірку послідовності 10^8 на випадковість за рахунок використання 19 методів оцінки випадковості, які формують 189 математичних «атак» на випадковість.

У табл. 1 наведені результати досліджень статистичних властивостей запропонованих методів на основі пакета *NIST STS* 822 [21].

Таблиця 1

Результати дослідження статистичної безпеки

Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99 % послідовностей	Кількість тестів, в яких тестування пройшли більше 96 % послідовностей	Кількість тестів, в яких тестування пройшли менше 96 % послідовностей
ССС Мак-Еліса на *ЕС*	149 (78,3 %)	189 (100 %)	0 (0 %)
SCCC R-N на скорочених *МЕС*	149 (78,8 %)	189 (100 %)	0 (0 %)
SCCC R-N на подовжених *МЕС*	150 (79,3 %)	189 (100 %)	0 (0 %)
SCCC R-N подовжених *МЕС+FC*	151 (79,9 %)	189 (100 %)	0 (0 %)
SCCC R-N скорочених *МЕС+ FC*	153 (80 %)	189 (100 %)	0 (0 %)

Аналіз табл.1 підтверджує рівень стійкості гібридних (комплексних) крипто-кодових конструкцій Рао-Нама та можливість їх використання в мобільних та смарт-технологіях.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропонована SCCC R-N/SMCCC R-N на алгеброгеометричних та збиткових кодах здатна забезпечити необхідний рівень безпеки, швидкість криптоперетворень та завадостійкість.

Використання різних класів завадостійких кодів забезпечує можливість додаткових переваг. По-перше, є можливість забезпечити використання SCCC R-N/SMCCC R-N на тому, чи іншому циклічному коді з урахуванням вимог щодо криптостійкості криптограми, а також часу безпеки криптограми. Крім цього, є можливість враховувати кількісну оцінку рівня секретності інформації.

Запропоновані симетричні криптосистеми забезпечують відповідний рівень безпеки в умовах появи повномасштабного комп’ютера, при цьому зберігаються відповідні вимоги щодо оперативності (швидкості криптоперетворень), а також інтегровано забезпечується підвищення рівня вірогідності за рахунок використання завадостійкого кодування.

Використання гібридних (комплексних) систем безпеки – HCCC R-N/HMCCC R-N, дозволяє значно скоротити обчислювальну складність практичного використання у mesh-мережах на основі смарт-технологій у поєднанні з бездротовими технологіями побудови каналів передачі. Це забезпечує практичне використання такого підходу у будь-якої системі безпеки

Таким чином, запропоновані симетричні постквантові криптосистеми забезпечують основні вимоги щодо безпеки передачі, зберігання інформації, а також є перспективним напрямом забезпечення всіх послуг безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207
2. Yevseiev, S., et al. (2021). Development of a conception for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies, 3*(9(111)), 63–83.
3. Petrivskyi, V., Shevchenko, V., Yevseiev, S., Milov, O., Laptiev, O., Bychkov, O., Fedoriienko, V., Tkachenko, M., & Opirskyy, I. (2022). Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. *Eastern-European Journal of Enterprise Technologies, 1*(9(115)), 15–23.
4. Yevseiev, S., Milevskyi, S., Bortnik, L., Voropay, A., Bondarenko, K., & Pohasii, S. (2022). Socio-cyber-physical systems security concept. In *Proceedings of the 4th International Congress on Human–Computer Interaction, Optimization and Robotic Applications (HORA 2022)* (June 9–11, 2022). Ankara, Turkey.
5. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography* (pp. 1–14). Springer.
6. Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016* (Lecture Notes in Computer Science, Vol. 9606, pp. 29–43). Springer.
7. Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., & Schanck, J. (2016). Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. *arXiv*. https://arxiv.org/abs/1603.09383
8. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report, 42*(44), 114–116.
9. Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory, 15*(2), 159–166.
10. Rao, T. R. N., & Nam, K. H. (1987). Private-key algebraic-code cryptosystems. In A. M. Odlyzko (Ed.), *Advances in cryptology – CRYPTO '86* (pp. 35–48). Springer. https://doi.org/10.1007/3-540-47721-7_3
11. Struik, R., & Van Tilburg, J. (1987). The Rao–Nam scheme is insecure against a chosen-plaintext attack. In *CRYPTO '87 Rump Session*.
12. Li, Y. X., Deng, R. H., & Wang, X. M. (1994). On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory, 40*(1), 271–273. https://doi.org/10.1109/18.272485
13. Bernstein, D. J. (2010). Grover vs. McEliece. In *Post-quantum cryptography* (pp. 73–80). Springer.
14. Sidelnikov, V. M. (1994). A public-key cryptosystem based on binary Reed–Muller codes. *Discrete Mathematics and Applications, 4*(3), 191–208.
15. Minder, L., & Shokrollahi, A. (2007). Cryptanalysis of the Sidelnikov cryptosystem. In *Advances in Cryptology – EUROCRYPT 2007* (pp. 347–360). Springer.
16. Baldi, M., & Chiaraluce, F. (2007). Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2007)* (pp. 2591–2595). IEEE.
17. Liu, J., Tong, X., Wang, Z., Ma, J., & Yi, L. (2019). An improved Rao–Nam cryptosystem based on fractional-order hyperchaotic system and EDF–QC–LDPC. *International Journal of Information Security*. https://doi.org/10.1142/S0218127419501220
18. Melenti, Y., Korol, O., Shulha, V., Milevskyi, S., Sievierinov, O., Voitko, O., Rzayev, K., Husarova, I., Kravchenko, S., & Pashayeva, S. (2025). Development of post-quantum cryptosystems based on the Rao–Nam scheme. *Eastern-European Journal of Enterprise Technologies, 1*(9(133)), 35–48. https://doi.org/10.15587/1729-4061.2025.323195
19. Yevseiev, S., et al. (2018). Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes. *Eastern-European Journal of Enterprise Technologies, 6*(4(96)), 24–31.
20. Yevseiev, S., Kots, H., & Liekariev, Y. (2016). Development of a multi-factor authentication method based on the Niederreiter–McEliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies, 6*(4(84)), 11–23.
21. Couvreur, A., Otmani, A., & Tillich, J.-P. (2014). Polynomial-time attack on wild McEliece over quadratic extensions. In *Advances in Cryptology – EUROCRYPT 2014* (pp. 17–39). Springer.
22. Yevseiev, S., et al. (2017). Construction of hybrid security systems based on crypto-code structures and flawed codes. *Eastern-European Journal of Enterprise Technologies, 4*(9(88)), 4–20.
23. Yevseiev, S., et al. (2019). Development of Niederreiter hybrid crypto-code structures on flawed codes. *Eastern-European Journal of Enterprise Technologies, 1*(9(97)), 27–37.

24. Dinh, H., Moore, C., & Russell, A. (2011). McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In P. Rogaway (Ed.), *Advances in Cryptology – CRYPTO 2011* (Lecture Notes in Computer Science, Vol. 6841). Springer. https://doi.org/10.1007/978-3-642-22792-9_43
25. Tsyhanenko, O., Rzayev, K., & Mammadova, T. (2018). Mathematical model of the modified Niederreiter crypto-code structures. *Advanced Information Systems*, *2*(4), 37–44.
26. Melenti, Y. O., & Laptiev, O. O. (2025). A model of hybrid threats to critical infrastructure facilities of the EU and Ukraine. *Proceedings of the National Academy of the Security Service of Ukraine*, 94, 78–89.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Sergii Dunaiev
Cybersecurity Department
National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine
ORCID: 0000-0001-8736-3602
serg.dynaev@gmail.com

DEVELOPMENT OF CRYPTOCODE CONSTRUCTIONS BASED ON ALGEBRAIC, LDPC, AND DAMAGE CODES

Abstract. The development of post-quantum technologies calls into question the cryptographic strength of modern symmetric and asymmetric cryptosystems. With the advent of a full-scale quantum computer, such systems will not be able to provide the required level of cryptographic strength (level 5 according to the US NIST scale). The competition of post-quantum algorithms has revealed a tendency towards the construction of cryptosystems based on the synthesis (integration) of security theories with Galois theory. Among the winners of post-quantum algorithms are the crypto-code constructions (CCC) of McEliece and Niederreiter, which make it possible to comprehensively provide the necessary level of protection and increase the level of probability of information transfer. But a significant drawback is the possibility of hacking such systems using linear codes, as well as the need to build them on the Galois field 2^{10}–2^{13}, which significantly reduces their ability to build systems based on intelligent technologies and mesh networks. The work proposes the use of symmetric CCC (SCCC) based on the Rao-Nama scheme (SCCC R-N) on MEC (modified elliptic codes), LDPC, and damage codes, which makes it possible to significantly reduce the volume of key data (constructing CCC using the Galois field 2^4–2^6) while maintaining the level of cryptographic strength of the probability of information transmission (the safe time is equal to the execution time of 10^{25}–10^{35} elementary group operations). This approach makes it possible to create intelligent information security systems (ISPS). The purpose of the research is to develop post-quantum algorithms based on the integration of theories for constructing cryptosystems of symmetric and asymmetric cryptography with methods for constructing error-resistant codes. This approach allows you to regulate the required level of stability of the cryptosystems based on the requirements for the secrecy of the information message, as well as the time it is stored, and the level of stability of the system as a whole.

Keywords: Rao-Nam crypto-code constructions, algebraic codes, LDPC, and defective codes.

REFERENCES

1. National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207
2. Yevseiev, S., et al. (2021). Development of a conception for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, *3*(9(111)), 63–83.
3. Petrivskyi, V., Shevchenko, V., Yevseiev, S., Milov, O., Laptiev, O., Bychkov, O., Fedoriienko, V., Tkachenko, M., & Opirskyy, I. (2022). Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. *Eastern-European Journal of Enterprise Technologies*, *1*(9(115)), 15–23.
4. Yevseiev, S., Milevskyi, S., Bortnik, L., Voropay, A., Bondarenko, K., & Pohasii, S. (2022). Socio-cyber-physical systems security concept. In *Proceedings of the 4th International Congress on Human–Computer Interaction, Optimization and Robotic Applications (HORA 2022)* (June 9–11, 2022). Ankara, Turkey.
5. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography* (pp. 1–14). Springer.
6. Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016* (Lecture Notes in Computer Science, Vol. 9606, pp. 29–43). Springer.
7. Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., & Schanck, J. (2016). Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. *arXiv*. https://arxiv.org/abs/1603.09383
8. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report, 42*(44), 114–116.

9. Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory, 15*(2), 159–166.
10. Rao, T. R. N., & Nam, K. H. (1987). Private-key algebraic-code cryptosystems. In A. M. Odlyzko (Ed.), *Advances in cryptology – CRYPTO '86* (pp. 35–48). Springer. https://doi.org/10.1007/3-540-47721-7_3
11. Struik, R., & Van Tilburg, J. (1987). The Rao–Nam scheme is insecure against a chosen-plaintext attack. In *CRYPTO '87 Rump Session*.
12. Li, Y. X., Deng, R. H., & Wang, X. M. (1994). On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory, 40*(1), 271–273. https://doi.org/10.1109/18.272485
13. Bernstein, D. J. (2010). Grover vs. McEliece. In *Post-quantum cryptography* (pp. 73–80). Springer.
14. Sidelnikov, V. M. (1994). A public-key cryptosystem based on binary Reed–Muller codes. *Discrete Mathematics and Applications, 4*(3), 191–208.
15. Minder, L., & Shokrollahi, A. (2007). Cryptanalysis of the Sidelnikov cryptosystem. In *Advances in Cryptology – EUROCRYPT 2007* (pp. 347–360). Springer.
16. Baldi, M., & Chiaraluce, F. (2007). Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2007)* (pp. 2591–2595). IEEE.
17. Liu, J., Tong, X., Wang, Z., Ma, J., & Yi, L. (2019). An improved Rao–Nam cryptosystem based on fractional-order hyperchaotic system and EDF–QC–LDPC. *International Journal of Information Security*. https://doi.org/10.1142/S0218127419501220
18. Melenti, Y., Korol, O., Shulha, V., Milevskyi, S., Sievierinov, O., Voitko, O., Rzayev, K., Husarova, I., Kravchenko, S., & Pashayeva, S. (2025). Development of post-quantum cryptosystems based on the Rao–Nam scheme. *Eastern-European Journal of Enterprise Technologies, 1*(9(133)), 35–48. https://doi.org/10.15587/1729-4061.2025.323195
19. Yevseiev, S., et al. (2018). Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes. *Eastern-European Journal of Enterprise Technologies, 6*(4(96)), 24–31.
20. Yevseiev, S., Kots, H., & Liekariev, Y. (2016). Development of a multi-factor authentication method based on the Niederreiter–McEliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies, 6*(4(84)), 11–23.
21. Couvreur, A., Otmani, A., & Tillich, J.-P. (2014). Polynomial-time attack on wild McEliece over quadratic extensions. In *Advances in Cryptology – EUROCRYPT 2014* (pp. 17–39). Springer.
22. Yevseiev, S., et al. (2017). Construction of hybrid security systems based on crypto-code structures and flawed codes. *Eastern-European Journal of Enterprise Technologies, 4*(9(88)), 4–20.
23. Yevseiev, S., et al. (2019). Development of Niederreiter hybrid crypto-code structures on flawed codes. *Eastern-European Journal of Enterprise Technologies, 1*(9(97)), 27–37.
24. Dinh, H., Moore, C., & Russell, A. (2011). McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In P. Rogaway (Ed.), *Advances in Cryptology – CRYPTO 2011* (Lecture Notes in Computer Science, Vol. 6841). Springer. https://doi.org/10.1007/978-3-642-22792-9_43
25. Tsyhanenko, O., Rzayev, K., & Mammadova, T. (2018). Mathematical model of the modified Niederreiter crypto-code structures. *Advanced Information Systems, 2*(4), 37–44.
26. Melenti, Y. O., & Laptiev, O. O. (2025). A model of hybrid threats to critical infrastructure facilities of the EU and Ukraine. *Proceedings of the National Academy of the Security Service of Ukraine*, 94, 78–89.