УДК 004.056.523
DOI: 10.31673/2409-7292.2025.041216

Стеценко В. О.

РОЗРОБКА МЕТОДІВ АВТЕНТИФІКАЦІЇ НА ОСНОВІ МОДИФІКОВАНИХ ТЕОРЕТИКО-КОДОВИХ СХЕМ

Розробка методів автентифікації є ключовим елементом сучасних криптографічних систем, що застосовуються для забезпечення безпеки передачі даних, цифрових підписів та захисту конфіденційної інформації. Одним з найбільш поширених підходів є використання традиційних алгоритмів RSA та ECC, стандартизованих у рекомендаціях NIST [1, 2]. Дані алгоритми відрізняються високою криптографічною стійкістю у класичних обчислювальних середовищах та гнучкістю завдяки підтримці різних математичних структур, що робить їх затребуваними в державних та комерційних системах захисту інформації. Проведений аналіз показав, що, незважаючи на низку переваг, RSA та ECC мають суттєві недоліки. Серед них – уразливість до квантових атак, зокрема алгоритму Шора, підвищені обчислювальні витрати для великих ключових даних та критична залежність від якості випадкових даних. Найбільш значима проблема полягає в відсутності стійкості до квантових обчислень, що ускладнює оцінку їх характеристик та знижує передбачуваність роботи в критичних криптографічних додатках. Для усунення виявлених обмежень запропоновано два варіанти методів автентифікації на основі модифікованих теоретко-кодових схем McEliece та Niederreiter. У їх структуру включено алгеброгеометричні коди, що дозволяє формально визначити мінімальну довжину циклу послідовності та забезпечити її гарантований період. Додаткові алгоритмічні процедури ускладнюють аналіз внутрішніх станів методів, підвищуючи їх криптостійкість. У статті представлено структурні схеми запропонованих методів, описано етапи їх функціонування та ключові аналітичні залежності, що визначають процес формування автентифікаційних даних. Розроблені підходи зберігають криптографічну стійкість традиційних схем, забезпечуючи при цьому постквантову безпеку та покращені можливості управління параметрами автентифікації. Отримані результати можуть бути використані при створенні програмно-апаратних засобів захисту інформації та криптографічних протоколів, що вимагають високої надійності та передбачуваності роботи систем автентифікації.

Ключові слова: методи автентифікації, теоретико-кодові схеми Мак-Еліса, теоретико-кодові схеми Нідерайтера, захист інформації, кібербезпека, загрози.

Вступ

У цифровому середовищі стрімкий розвиток квантових технологій створює серйозні виклики для традиційних криптографічних систем. Алгоритми RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography), базуються на складних математичних задачах (факторизація великих чисел та обчислення дискретних логарифмів), які стають уразливими перед алгоритмом Шора, реалізованим на квантових комп'ютерах [3]. Це загрожує безпеці систем автентифікації та авторизації, що використовують цифрові підписи та сертифікати. Постквантова криптографія (PQC) пропонує нові підходи, зокрема на основі теорії кодування, які стійкі до квантових атак. У цьому контексті особливого значення набувають модифіковані криптосистеми McEliece та Niederreiter. Ця стаття досліджує розробку методів автентифікації на основі таких схем, акцентуючи увагу на їх практичній реалізації та інтеграції в системи захисту інформації.

Аналіз літературних джерел та формулювання проблеми

Дослідження в галузі постквантової криптографії (PQC) активно проводяться з 1978 року, коли R.J. McEliece запропонував криптосистему на основі алгебраїчних кодів [5]. Ця робота поклала основу для теоретико-кодових криптосистем, які стійкі до квантових атак завдяки NP-складним задачам декодування. Подальші розробки, зокрема Niederreiter у 1986 році, розвинули ідеї, інтегруючи їх з теорією кодування для створення варіацій, подібних до McEliece, з фокусом на шифрування через додавання контрольованого шуму [6]. У сучасних публікаціях, таких як [7], акцент робиться на модифікації цих схем із використанням еліптичних та алгеброгеометричних кодів, що підвищує ефективність у системах автентифікації та шифрування. NIST активно просуває стандартизацію PQC, виділяючи алгоритми на основі ґрат (Kyber, Dilithium), багаточленів (Rainbow) та хеш-функцій. (SPHINCS+) [8]. У 2022–2025 роках NIST завершив третій і четвертий раунди стандартизації, обравши п'ять основних алгоритмів: ML-KEM, ML-DSA, SLH-DSA, FALCON (FN-DSA) [9].

Проведений аналіз показує, що генератори псевдовипадкових чисел, такі як LFSR, ефективні для формування інформаційних послідовностей у цих схемах, але їх лінійність робить вразливими до криптоаналізу, вимагаючи інтеграції з нелінійними S-блоками для підвищення стійкості. Дослідження 2025 року в arXiv акцентують на аналізі теоретико-кодових систем, як McEliece з кодами Goppa, порівнюючи їх з криптографією на основі грат (наприклад, NTRU), і відзначають переваги в стійкості до квантових атак, але з більшими обчислювальними витратами [10]. Незважаючи на прогрес, залишається відкритим питання оптимізації обчислювальних витрат, зокрема при визначенні матриці G у теоретико-кодових схемах, а також інтеграції з хеш-функціями для гібридних систем. Перспективи включають стандартизацію NIST 2025 року, де теоретико-кодові алгоритми, як HQC, виділяються для практичного впровадження [11].

Постановка проблеми

Стрімкий розвиток квантових технологій робить алгоритми RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography) вразливими. Алгоритм Шора [4], дозволяє квантовими комп'ютерами розв'язувати задачі які використовують данні алгоритми в поліноміальний час, тоді як на класичних комп'ютерах це вимагає експоненціальних ресурсів. Аналогічно, ECC вразлива до алгоритма Шора через залежність від дискретного логарифму в еліптичних кривих. Алгоритм Гровера посилює загрозу, прискорюючи пошукові задачі, що впливає на симетричні шифри та хеш-функції, хоча основна небезпека для асиметричних алгоритмів – від Шора. Це ставить під загрозу глобальну інфраструктуру. Необхідність розробки постквантових методів автентифікації, стійких до алгоритмів Шора та Гровера, є нагальною.

Мета роботи та цілі дослідження

Метою статті є розробка методів автентифікації на основі модифікованих теоретико-кодових схем McEliece та Niederreiter з використанням алгеброгеометричних кодів) над полем $GF(2^4)$.

Виклад основного матеріалу

В якості основи для розробки методу автентифікації на крипто-кодовій конструкції McEliece обрана Challenge-response аутентифікація [12].

Схематично запропонований метод автентифікації заснований на крипто-кодовій конструкції McEliece представлено на рисунку 1.

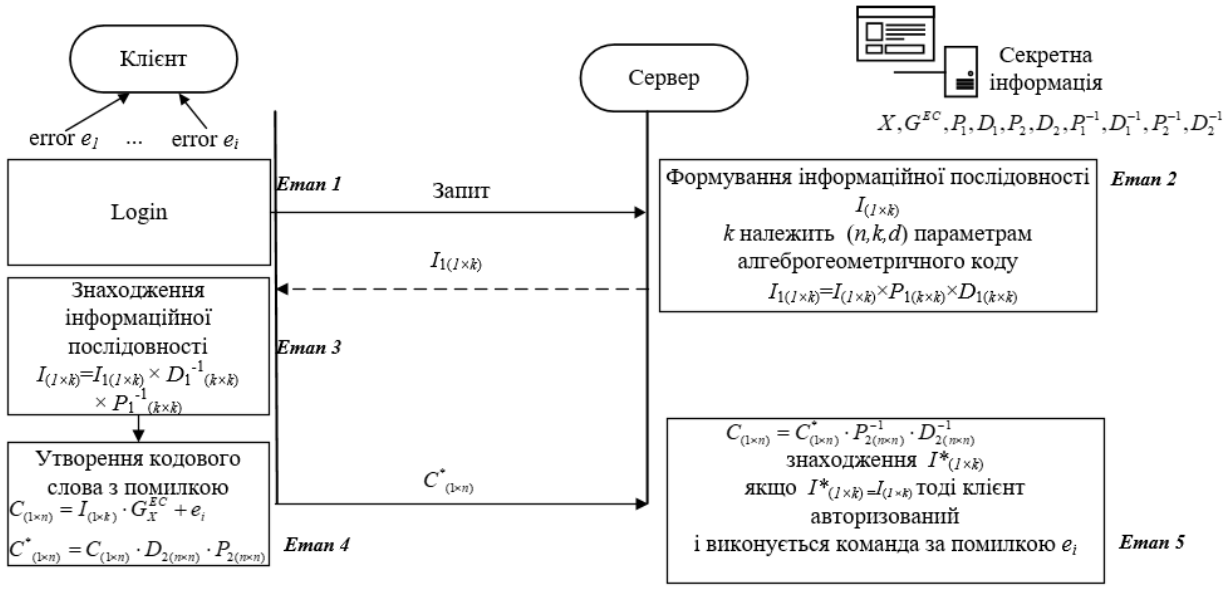

Рис.1. Метод автентифікації заснований на модифікованій крипто-кодовій конструкції McEliece

Запропонований метод автентифікації складається з наступних кроків:

– на *першому* етапі як і в Challenge-response аутентифікаціі проводиться ініціювання запиту (Challenge), на даному етапі система надсилає користувачеві випадково згенероване значення чи питання. Цей запит може бути надісланий на пристрій клієнта або на екрані входу;

– на *другому* етапі проводиться формування інформаційної послідовності $I_{(1\times k)}$ з елементами *GF(q)*, для формування даної послідовності в статті пропонується використовувати генератори псевдовипадкових чисел які будуть розглянуті далі. За рахунок використання перестановочної ($P_{1(k\times k)}$) та діагональної матриць ($D_{1(k\times k)}$) які зберігаються в секреті, формується інформаційна послідовність $I_{1(1\times k)} = I_{(1\times k)} \times P_{1(k\times k)} \times D_{1(k\times k)}$ як відповідь на запит;

– на *третьому* етапі по отриманій інформаційній послідовності $I_{1(1\times k)} = = I_{(1\times k)} \times P_{1(k\times k)} \times D_{1(k\times k)}$ за рахунок використання зворотних перестановочної ($P^{-1}_{1(k\times k)}$) та діагональної матриць ($D^{-1}_{1(k\times k)}$)) отримуємо інформаційну послідовність $I_{(1\times k)} = = I_{1(1\times k)} \times D^{-1}_{1(k\times k)} \times P^{-1}_{1(k\times k)}$;

– на *четвертому* етапі проводиться формування кодового слова з помилками $C_{(1\times n)} = I_{(1\times k)} \times G^{EC}_{X} + e_i$ в якому помилка e_i визначає виконання тієї чи іншої операції. За рахунок використання перестановочної ($P_{2(n\times n)}$) та діагональної матриць ($D_{2(n\times n)}$) які зберігаються в секреті, формується кодова послідовність $C^*_{(1\times n)} = C_{(1\times n)} \times D_{2(n\times n)} \times P_{2(n\times n)}$;

– на *п'ятому* етапі по отриманій послідовності $C^*_{(1\times n)} = C_{(1\times n)} \times D_{2(n\times n)} \times P_{2(n\times n)}$ проводиться зворотне перетворення $C_{(1\times n)} = C^*_{(1\times n)} \times P^{-1}_{2(n\times n)} \times D^{-1}_{2(n\times n)}$ і по відомому кодовому слову без помилок визначається інформаційне повідомлення I*$_{(1\times k)}$ та помилка e_i. Якщо отримане повідомлення $I^*_{(1\times k)}$ дорівнює $I_{(1\times k)}$ яке було сформовано на другому етапі то користувач визначається автоматизованим та виконується операція яка дорівнює помилці e_i.

Схема Niederreiter є варіацією криптосистем на основі кодів, подібних до криптосистеми McEliece [6], вона використовує ідею шифрування повідомлень шляхом їхнього перетворення на кодові слова коректуючого коду, з подальшим додаванням контрольованого шуму. Задача декодування в цьому контексті є складною математичною проблемою, що забезпечує стійкість криптосистеми.

Схематично запропонований метод автентифікації заснований на модифікованій крипто-кодовій конструкції Niederreiter представлено на рисунку 2.

Запропонований метод автентифікації складається з наступних кроків:

– на *першому* етапі як і в Challenge-response аутентифікаціі проводиться ініціювання запиту (Challenge), на даному етапі система надсилає користувачеві випадково згенероване значення чи питання. Цей запит може бути надісланий на пристрій клієнта або на екрані входу;

– на *другому* етапі за запитом формується інформаційна послідовність $I_{(1\times k)}$ з виходу генератора псевдовипадкових чисел за рахунок використання *S* блоків. Формування інформаційній послідовності $I_{(1\times k)}$ буде розглянуто далі. По відомій інформаційній послідовності $I_{(1\times k)}$ проходить процес формування кодового слова без помилок $C_{(1\times n)} = I_{(1\times k)} \times G_{(k\times n)}$. За рахунок використання перестановочної $P_{(n\times n)}$ та діагональної матриць

$D_{(n\times n)}$ які зберігаються в секреті, формується кодове слово $C^*_{(1\times n)} = C_{(1\times n)} \times P_{(n\times n)} \times D_{(n\times n)}$ як відповідь на запит;

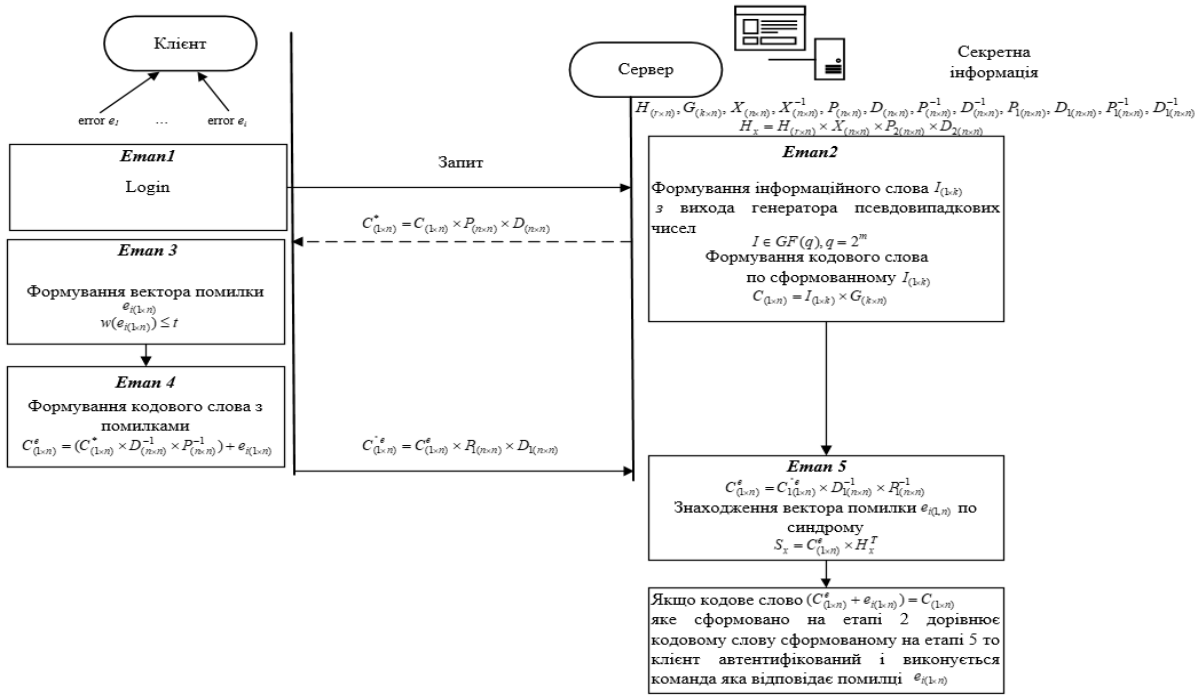

Рис. 2. Метод автентифікації заснований на модифікованій крипто-кодовій конструкції Niederreiter

– на *третьому* етапі проводиться формування вектору помилок $e_{i(1\times n)}$ вагою $w(e_{i(1\times n)}) \le t$;

– на *четвертому* етапі формується кодове слово з помилками $C^e_{(1\times n)} = (C^*_{(1\times n)} \times D^{-1}_{(n\times n)} \times P^{-1}_{(n\times n)}) + e_{i(1\times n)}$. Сформоване кодове слово $C^e_{(1\times n)} = (C^*_{(1\times n)} \times D^{-1}_{(n\times n)} \times P^{-1}_{(n\times n)}) + e_{i(1\times n)}$ з помилками для попередження компрометації при передачі по відкритому каналу зв'язку множиться на перестановочну і діагональну матриці $C^{*e}_{(1\times n)} = C^e_{(1\times n)} \times P_{1(n\times n)} \times D_{1(n\times n)}$;

– На *п'ятому* етапі проводиться зворотне перетворення $C^e_{(1\times n)} = C^{*e}_{1(1\times n)} \times D^{-1}_{1(n\times n)} \times P^{-1}_{1(n\times n)}$ і визначається синдром $S_x = C^e_{(1\times n)} \times H^T_x$ який відповідає помилці $e_{i(1\times n)}$. Якщо кодове слово $C_{(1\times n)}$ яке сформовано на етапі 2 дорівнює кодовому слову сформованому на етапі 5 $(C^e_{(1\times n)} + e_{i(1\times n)})$ то клієнт автентифікований і виконується команда яка відповідає помилці $e_{i(1\times n)}$.

На другому етапі запропонованих методів автентифікації для формування інформаційної послідовності $I_{(1\times k)}$ з елементами GF(q) пропонується використовувати генератори псевдовипадкових чисел.

Для формування інформаційної послідовності $I_{(1\times k)}$ для запропонованих схем автентифікації на основі крипто-кодових криптосистем Niederreiter та McEliece в статті пропонується використовувати генератори псевдовипадкових чисел на основі регістрів зсуву з лінійним зворотнім зв'язком. Інформаційна послідовність $I_{(1\times k)}$ представляє собою матрицю

яка складається з однієї строки та *k* стовпців в яких знаходяться елементи поля $GF(2^m)$ в залежності від *(n,k,d)* параметрів коду який буде використовуватися в алгоритмі McEliece са або Niederreite. Порядок формування інформаційної послідовності $I_{(1\times k)}$ представлено на рисунку 3.

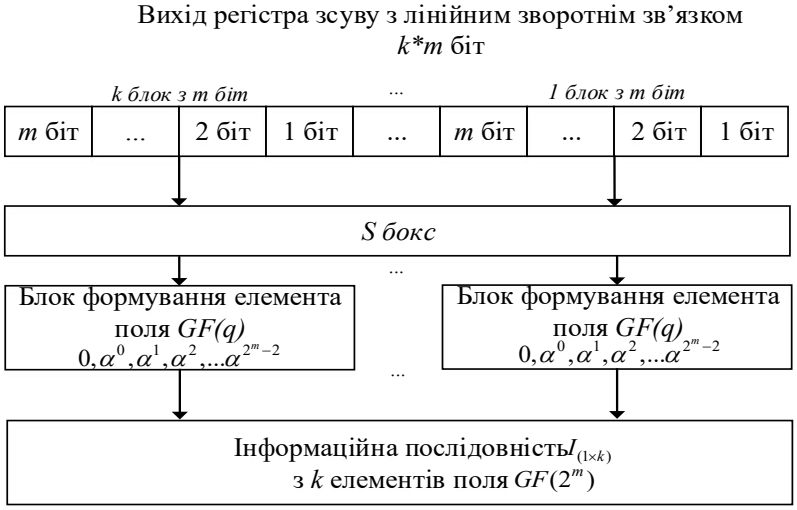

Рис. 3. Схема формування інформаційної послідовності $I_{(1\times k)}$

Схема формування інформаційної послідовності $I_{(1\times k)}$ працює наступним чином. За запитом формується інформаційна послідовність $I_{(1\times k)}$ з виходу генератора псевдовипадкових чисел на основі регістрів зсуву з лінійним зворотнім зв'язком. Значення реєстру здвигу з лінійним зворотнім зв'язком розбивається на блоки по *m* біт (*m* залежіть від параметрів *(n, k, d)* коду.

Таблиця 1

Приклад роботи блок формування елемента для поля $GF(2^4)$

№ з/п	Вхід блоку формування елемента поля $GF(2^4)$	Вихід з блоку формування елемента поля $GF(2^4)$
1	0000	0
2	0001	α^0
3	0010	α^1
4	0011	α^2
5	0100	α^3
6	0101	α^4
7	0110	α^5
8	0111	α^6
9	1000	α^7
10	1001	α^8
11	1010	α^9
12	1011	α^{10}
13	1100	α^{11}
14	1101	α^{12}
15	1110	α^{13}
16	1111	α^{14}

Кількість блоків залежить від виправляючої здатності алгебраїчного *(n, k, d)* коду. Використання S-блоку вносить нелінійне перетворення в процес шифрування, що ускладнює криптоаналіз, зокрема лінійний та диференціальний та реалізує принцип "змішування", запропонований Шенноном, щоб приховати зв'язок між відкритим текстом, шифротекстом і ключем. Робота блока формування елемента поля в самому простому вигляді представлено в таблиці 1.

Далі над сформованою послідовністю $I_{(1\times k)}$ проводяться математичні операції додавання та множення згідно алгоритмів представлених на рисунку 1,2.

Для забезпечення послуг автентифікації в статті пропонується використовувати алгеброгеометричний код з наступними *(n, k, d)* парметрами, *n=25, k=19, d=3* з елементами поля $GF(2^4)$. Запропонований алгеброгеометричний код *(25,19,3)* дозволяє виправити одну помилку ($d = 2t + 1 = 3$). Для формування інформаційної послідовність $I_{(1\times 19)}$ необхідно використовувати регістр зсуву довжиною 76 біт який будується за модулем непривідного багаточлена 76 ступеня. В якості приклада можна використати наступні многочлені: $g(x) = x^{76} + x^5 + 1;\ g(x) = x^{76} + x^{21} + x^{19} + x^1 + 1.$

Дані генератори псевдовипадкових чисел генерують послідовність максимального періоду і просто реалізуються як апаратно, так і програмно.

Порядок формування інформаційної послідовності $I_{(1\times 19)}$ з елементами поля $GF(2^4)$ представлено на рисунку 4.

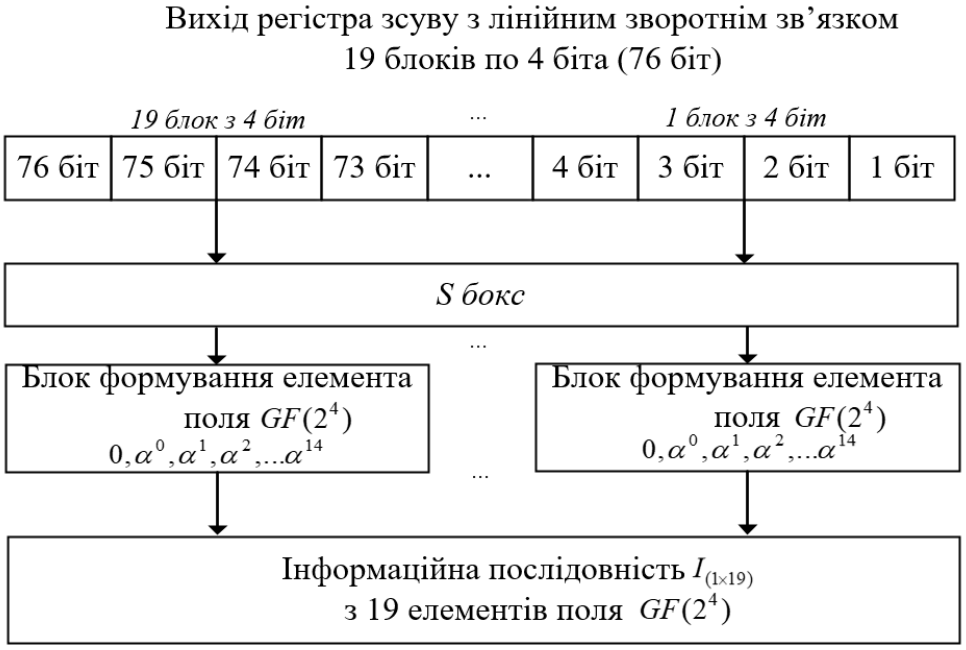

Рис. 4. Схема формування інформаційної послідовності $I_{(1\times 19)}$ з елементами поля $GF(2^4)$

Запропонований метод автентифікації на основі модифікованої крипто-кодової криптосистеми McEliece складається з наступних кроків:

– на *першому* етапі як і в Challenge-response аутентифікації проводиться ініціювання запиту (Challenge), на даному етапі система надсилає користувачеві випадково згенероване значення чи питання. Цей запит може бути надісланий на пристрій клієнта або на екрані входу;

– на *другому* етапі проводиться формування інформаційної послідовності $I_{(1\times 19)}$ з елементами *GF(2⁴)*. Процес формування інформаційної послідовності $I_{(1\times 19)}$ представлено на

рисунку 4. За рахунок використання перестановочної ($P_{1(19\times19)}$) та діагональної матриць ($D_{1(19\times19)}$) які зберігаються в секреті, формується інформаційна послідовність $I_{1(1\times19)} = I_{(1\times19)} \times P_{1(19\times19)} \times D_{1(19\times19)}$ як відповідь на запит;

– на *третьому* етапі по отриманій інформаційній послідовності $I_{1(1\times19)} = I_{(1\times19)} \times P_{1(19\times19)} \times D_{1(19\times19)}$ за рахунок використання зворотних перестановочної $P^{-1}_{1(19\times19)}$ та діагональної матриць $D^{-1}_{1(19\times19)}$ отримуємо інформаційну послідовність $I_{(1\times19)} = I_{1(1\times19)} \times D^{-1}_{1(19\times19)} \times P^{-1}_{1(19\times19)}$;

– на *четвертому* етапі проводиться формування кодового слова з помилками $C_{(1\times25)} = I_{(1\times19)} \cdot G^{EC}_X + e_i$ в якому помилка $e_{i(1\times19)}$ визначає виконання тієї чи іншої операції. За рахунок використання перестановочної ($P_{2(25\times25)}$) та діагональної матриць (D*2(25×25)*) які зберігаються в секреті, формується кодова послідовність $C^*_{(1\times25)} = C_{(1\times25)} \cdot D_{2(25\times25)} \cdot P_{2(25\times25)}$;

– на *п'ятому* етапі по отриманій послідовності $C^*_{(1\times25)} = C_{(1\times25)} \cdot D_{2(25\times25)} \cdot P_{2(25\times25)}$ проводиться зворотне перетворення $C_{(1\times25)} = C^*_{(1\times25)} \cdot P^{-1}_{2(25\times25)} \cdot D^{-1}_{2(25\times25)}$ і по відомому кодовому слову $C_{(1\times25)} = C^*_{(1\times25)} \cdot P^{-1}_{2(25\times25)} \cdot D^{-1}_{2(25\times25)}$ визначається інформаційне повідомлення $I^*_{(1\times19)}$ та помилка $e_{i(1\times19)}$. Якщо отримане повідомлення $I^*_{(1\times19)}$ дорівнює $I_{(1\times19)}$ яке було сформовано раніше на другому етапі то користувач визначається авторизованим та виконується операція яка дорівнює помилці $e_{i(1\times19)}$.

Схематично запропонований метод автентифікації заснований на модифікованій крипто-кодовій конструкції McEliece представлено на рисунку 5.

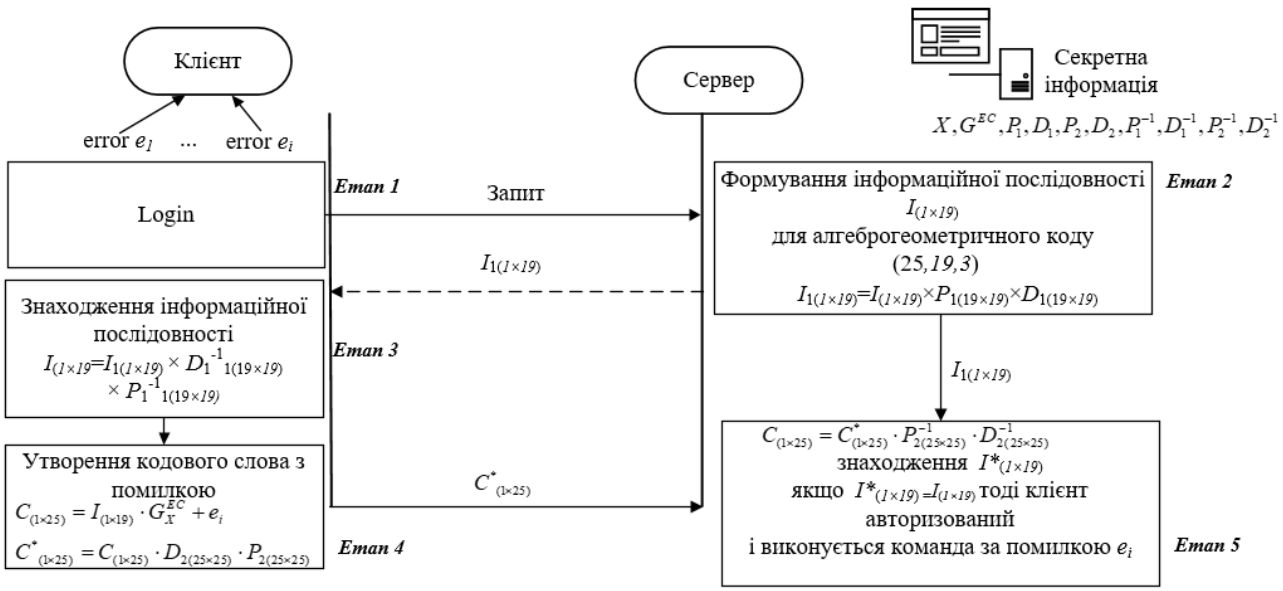

Рис. 5. Метод автентифікації заснований на модифікованій крипто-кодовій конструкції McEliece для алгеброгеометричного коду (25,19,3)

© Стеценко В. О. (2025) Розробка методів автентифікації на основі модифікованих теоретико-кодових схем. Сучасний захист інформації, 4(64), 155–164.
https://doi.org/10.31673/2409-7292.2025.041216

Схематично запропонований метод автентифікації заснований на модифікованій крипто-кодовій конструкції Niederreite на основі алгеброгеометричного коду (25,19,3) представлено на рисунку 6.

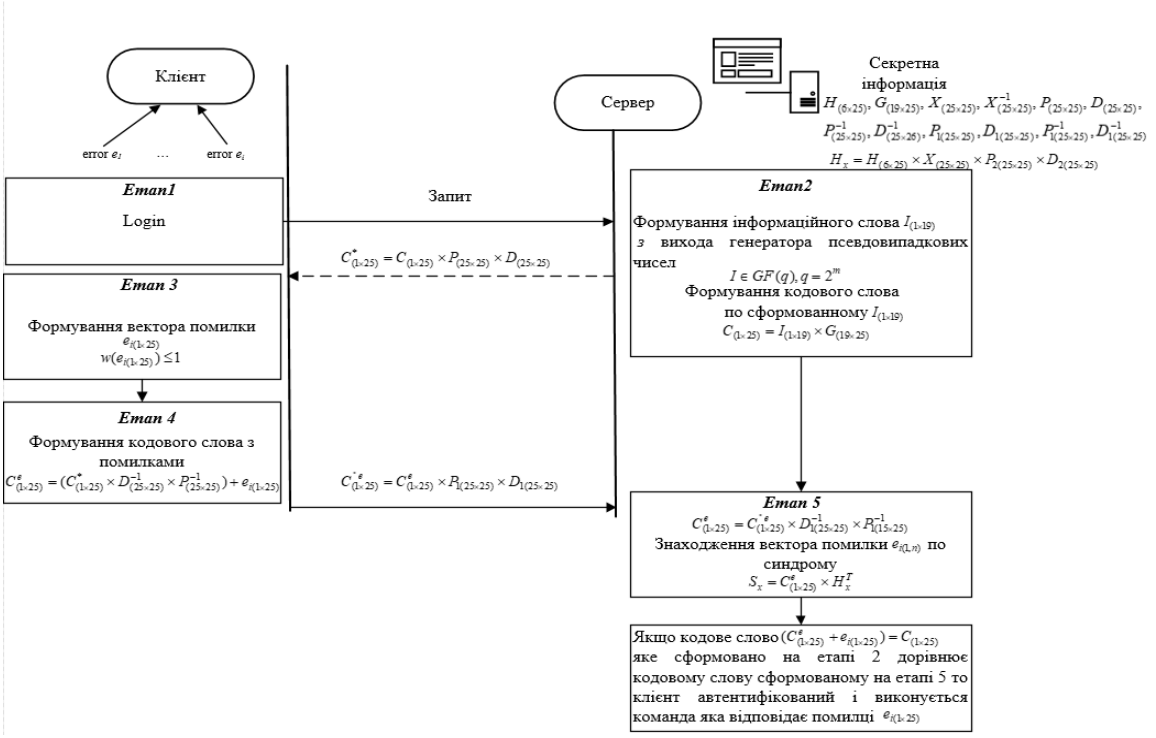

Рис. 6. Метод автентифікації заснований на модифікованій крипто-кодовій конструкції Niederreite

Запропонований метод автентифікації складається з наступних кроків:

– на *першому* етапі як і в Challenge-response аутентифікації проводиться ініціювання запиту (Challenge), на даному етапі система надсилає користувачеві випадково згенеровано значення чи питання. Цей запит може бути надісланий на пристрій клієнта або на екрані входу;

– на *другому* етапі за запитом формується інформаційна послідовність $I_{(1\times19)}$ з виходу генератора псевдовипадкових чисел за рахунок використання S блоків. По відомій інформаційній послідовності $I_{(1\times19)}$ проходить процес формування кодового слова без помилок $C_{(1\times25)} = I_{(1\times19)} \times G_{(19\times25)}$. За рахунок використання перестановочної $P_{(25\times25)}$ та діагональної матриць $D_{(25\times25)}$ які зберігаються в секреті, формується кодове слово для попередження компрометації при передачі по відкритому каналу зв'язку $C^*_{(1\times25)} = C_{(1\times25)} \times P_{(25\times25)} \times D_{(25\times25)}$ як відповідь на запит;

– на *третьому* етапі проводиться формування вектору помилок $e_{i(1\times25)}$ вагою $w(e_{i(1\times n)}) = 1$;

– на *четвертому* етапі формується кодове слово з помилками $C^e_{(1\times25)} = (C^*_{(1\times25)} \times D^{-1}_{(25\times25)} \times P^{-1}_{(25\times25)}) + e_{i(1\times25)}$. Сформоване кодове слово $C^e_{(1\times25)} = (C^*_{(1\times25)} \times D^{-1}_{(25\times25)} \times P^{-1}_{(25\times25)}) + +e_{i(1\times25)}$ з помилками для попередження компрометації при передачі по відкритому каналу зв'язку множиться на перестановочну і діагональну матриці $C^{*e}_{(1\times25)} = C^e_{(1\times25)} \times P_{1(25\times25)} \times D_{1(25\times25)}$.

– на *п'ятому* етапі проводиться зворотне перетворення $C^{e}_{(1\times25)} = C^{*e}_{1(1\times25)} \times$ $\times D^{-1}_{1(25\times25)} \times P^{-1}_{1(25\times25)}$ і визначається синдром $S_x = C^{e}_{(1\times25)} \times H^{T}_{x}$ який відповідає помилці $e_{i(1\times25)}$. Якщо кодове слово $C_{(1\times25)}$ яке сформовано на етапі 2 дорівнює кодовому слову сформованому на етапі 5 $(C^{e}_{(1\times25)} + e_{i(1\times25)})$ то клієнт автентифікований і виконується команда яка відповідає помилці $e_{i(1\times25)}$.

Висновки і перспективи наступних досліджень

Розроблено метод автентифікації на основі модифікованій крипто-кодової конструкції McEliece. Запропоновано використання Challenge-Response автентифікації з алгебро-геометричними кодами *(25,19,3)* над полем $GF(2^4)$, що забезпечує постквантову стійкість до атак, включаючи формування інформаційної послідовності з маскуванням за допомогою перестановочних і діагональних матриць.

Розроблено метод автентифікації на основі модифікованій крипто-кодової конструкції Niederreiter. Запропонований метод включає генерацію вектору помилок і синдрому для перевірки автентичності, з використанням алгеброгеометричного кода (25,19,3), що дозволяє виправляти помилки та виконувати команди, пов'язані з помилками, забезпечуючи захист від квантових загроз.

Запропоновано алгоритм формування інформаційної послідовності I, яка використовується у двох запропонованих алгоритмах автентифікації. Використання LFSR довжиною 76 біт за модулем неприводимого многочлена 76-го ступеня дає можливість формувати інформаційну послідовність $I_{(1\times19)}$ довжиною 19 елементів поля $GF(2^4)$, що дає можливість формувати кодове слово $C_{(1\times25)}$ яке в подальшому використовується в запропонованих методах автентифікації згідно теорії кодування.

Запропоновані методи на основі кодових криптосистем McEliece та Niederreiter стійкі до квантових атак (алгоритм Шора), на відміну від традиційних RSA та ECC, і дозволяють інтеграцію в системи захисту інформації з використанням алгеброгеометричних кодів для виправлення помилок. Запропоновані методи забезпечують високу криптостійкість і швидкість, але вимагають обчислення породжуючої матриці *G* за відомою перевірочною *H*, що є потенційним недоліком.

Перелік посилань

1. National Institute of Standards and Technology. NIST Special Publication. https://doi.org/10.6028/NIST.SP.800-56Ar3.

2. National Institute of Standards and Technology. NIST Special Publication. .https://doi.org/10.6028/NIST.SP.800-56Br2 .

3. Dustin Moody Post-Quantum Cryptography: NIST's Plan for the PQCrypto 2016 conference. Post-Quantum Cryptography 7th International Workshop, PQCrypto 2016 Fukuoka, Japan, February 24–26, 2016: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/pqcrypto-2016-presentation.pdf.

4. Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." In Proceedings 35th annual symposium on foundations of computer science, pp. 124-134. Ieee, 1994.

5. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Pro-pulsion Lab., Pasadena, CA, January-February, 1978. P. 114-116.

6. Niederreiter, H. Knapsack-type cryp-tosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. P. 19-34.

7. S. Yevseiev, O. Korol, and other, "Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes", Eastern-European Journal of Enterprise Technologies, 4, 9(82), p. 18 – 26, 2016

8. National Institute of Standards and Technology. NIST IR 8413 https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf.

9. Alexander Meyer Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems https://doi.org/10.48550/arXiv.2505.0879.

10. National Institute of Standards and Technology.NIST IR 8545: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf.

11. Dariusz Rzońca, Andrzej Stec, Bartosz Trybus Secure web access to mini distributed control system: Niewielkie rozproszone systemy sterowania ze zdalnym dostępem przez sieć January 2012, Automatyka/Automatics, 16(2) p. 155-164].

12. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., ...Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 – Proceedings. 2021. P. 67–70.

13. Serhii Yevseiev & Yuliia Khokhlachova & Serhii Ostapov & Oleksandr Laptiev et al, 2023. "Models of socio-cyber-physical systems security," Monographs, PC TECHNOLOGY CENTER, number 978-617-7319-72-5.redif, December. DOI: https://doi.org/10.15587/978-617-7319-72-5.

14. Oleksandr Laptiev, Volodymyr Tkachev, Oleksii Maystrov, Oleksandr Krasikov, Pavlo Open'ko, Volodimir Khoroshko, Lubomir Parkhuts. The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). 2021.Vol 13, No 2, August P.271-277. . DOI : https://doi.org/10.54039/ijcnis.v13i2.5008.

15. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022 P. 93–101. DOI: https://doi.org/10.15587/1729-4061.2022.253530.

16. Oleksandr Laptiev, Andrii Musienko, Volodymyr Nakonechnyi, Andrii Sobchuk, Sergii Gakhov, Serhii Kopytko. Algorithm for Recognition of Network Traffic Anomalies Based on Artificial Intelligence.5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 08-10 June 2023

17. DOI: https://doi.org/10.1109/HORA58378.2023.10156702.

Надійшла 21.11.2025

УДК 004.056.55
DOI: 10.31673/2409-7292.2025.041218

Цебак О.А., Войтусік С.С.

МЕТОДИ ОЦІНКИ ЯКОСТІ ТА КРИПТОСТІЙКОСТІ ПОСЛІДОВНОСТЕЙ, ЗГЕНЕРОВАНИХ ГЕНЕРАТОРАМИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

У статті проведено комплексний аналіз методів оцінки якості та криптостійкості генераторів псевдовипадкових чисел (ГПВЧ), які є ключовими елементами сучасних криптографічних систем. Розглянуто декілька основних груп підходів, серед яких статистичні, оцінка криптографічної стійкості, тощо. Статистичні методи, реалізовані у стандартах NIST, дозволяють визначити рівень випадковості послідовностей за такими критеріями, як рівномірність, відсутність кореляцій та ентропічна достатність. Натомість криптографічні підходи зосереджені на перевірці непередбачуваності та стійкості генератора до відновлення внутрішнього стану. Особливу увагу приділено ентропічному аналізу відповідно до вимог NIST SP 800-90B та впливу потенційних квантових атак, що зумовлюють необхідність перегляду існуючих моделей безпеки. Визначено, що жоден окремий метод не забезпечує повної оцінки надійності ГПВЧ, тому найбільш ефективним є комбінований підхід, який поєднує статистичні, криптоаналітичні та ентропічні методи. Запропоновано напрями подальшого розвитку оцінювальних методик, зокрема застосування алгоритмів машинного навчання для виявлення прихованих закономірностей, використання формальних математичних доказів безпеки та створення гібридних систем перевірки, здатних враховувати ризики постквантової криптографії. Отримані результати можуть бути використані для вдосконалення стандартів тестування генераторів та підвищення надійності криптографічних засобів захисту інформації.

Ключові слова: квантові обчислення, криптостійкість, генератори псевдовипадкових чисел, стандарти безпеки, криптографічні системи.

Вступ

Генератори псевдовипадкових чисел (ГПВЧ) є фундаментальним елементом сучасних криптографічних систем, оскільки від їхньої надійності та якості залежить стійкість шифрування, електронних підписів, протоколів автентифікації та інших механізмів захисту інформації. На відміну від звичайних застосунків, де достатньо забезпечити статистичну подібність послідовності до випадкової, у криптографії ключову роль відіграє саме