УДК 621.391

В. Грабчак, З. Грабчак[1]
Академія сухопутних військ,
[1]Харківський університет Повітряних сил

ОЦІНКА СКЛАДНОСТІ КОДОВИХ СХЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДОКАЗОВОЇ СТІЙКОСТІ НА ПРОСТОРОВИХ КРИВИХ

Розглянуто питання побудови кодової схеми захисту інформації Мак-Еліса з використанням алгеброгеометричних кодів на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних. Досліджено складності реалізації алгоритмів формування та декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих, оцінена часова й ємкісна складності функціонування цих алгоритмів.

Ключові слова: кодові схеми захисту інформації, схема Мак-Еліса, алгеброгеометричні коди на просторових кривих, алгоритми формування та декодування кодограм, часова й ємкісна складність.

This article deals with the problems of constructions of code chart of McEliece information protection with usage of algebra-geometrical codes on the spatial curves given in the descriptive space P^3 by the joint solutions of totality of two homogeneous equations from four variables. The research of complexity of realization of algorithms of forming and decoding of codegrams in a code chart of McEliece information protection with algebra-geometrical codes on the spatial curves is conducted, the time and capacious complexities of these algorithms functioning axe estimated.

Keywords: code chart of information protection, McEliece chart, algebra-geometrical codes on the spatial curves, algorithms of forming and decoding of codegrams, temporal and capacious complexity.

Вступ

Постановка проблеми в загальному вигляді та аналіз літератури. Сьогодні ймовірнісно-часові вимоги до телекомунікаційних систем спеціального призначення (ТССП) значно підвищилися. Це виражається насамперед у жорстких нормативах у вірогідності та інформаційній прихованості передавання даних в ТССП.

Проведений аналіз [1, 2] показав, що системи передачі формалізованих даних в існуючих ТССП не забезпечують зростаючих вимог. Одним із основних і найефективніших механізмів забезпечення потрібної вірогідності передавання даних у ТССП є завадостійке кодування [3, 4]. Задача підвищення інформаційної прихованості розв'язується методами спеціального перетворення інформації (шифрування) [5, 6]. Одним із перспективних напрямів є використання систем, які побудовані з використанням алгебраїчних блокових кодів, так звані кодові схеми захисту інформації доказової стійкості [7–9]. Їх застосування дає змогу, по-перше, будувати несиметричні алгоритми перетворення інформації, в яких не накладаються обмеження щодо секретності ключових даних, по-друге, поєднувати завадостійке кодування зі спеціальним перетворенням інформації. Це дає можливість інтегровано підвищувати вірогідність і інформаційну прихованість передачі даних у ТССП. Водночас відомі методи побудови кодових схем захисту інформації доказової стійкості не дають змогу повною мірою забезпечити потрібні показники. Так, у [10]

запропонований ефективний метод зламу схеми Мак-Еліса з кодом Ріда–Соломона. Там же автор висуває припущення про потенційну вразливість схем, які побудовані на узагальнених кодах Боуза–Чоудхурі–Хоквінгема. Крім того, процедури зламу схеми Мак-Еліса можуть бути легко трансформовані на схеми Нідеррайтера. Стійкість кодових схем захисту інформації, побудованих на кодах Ріда–Соломона і кодах Боуза–Чоудхурі–Хоквінгема, вважається недостатньою.

Одним із перспективних напрямів розвитку кодових схем захисту інформації доказової стійкості, спрямованих на підвищення стійкості, є використання алгеброгеометричних кодів на просторових кривих [11, 12]. Застосування кодів, побудованих за алгебраїчними кривими для формування кодових схем захисту інформації, дасть змогу отримати додатковий параметр маскування коду – вид алгебраїчної кривої, на основі якої будується перевіркова і породжувальна матриці коду.

Крім того, в роботах [13, 14] показано, що при інших рівних умовах використання алгеброгеометричних кодів дає змогу отримати найбільший енергетичний виграш від кодування і досягти високих показників вірогідності. Із збільшенням потужності алфавіту кодових символів і довжини коду енергетичний виграш збільшується.

Актуальним питанням функціонування кодових схем захисту інформації доказової стійкості на просторових кривих є дослідження складності їх формування і декодування кодограм, накладення і зняття ключових даних.

Мета статті

Метою статті є розроблення процедур функціонування кодової схеми захисту інформації Мак-Еліса з використанням алгеброгеометричних кодів на просторових кривих, оцінювання часової і ємнісної складності алгоритмів формування і декодування кодограм та оцінка їх асимптотичної складності.

Основна частина

Кодові схеми захисту інформації доказової стійкості. Розглянемо кодову схему захисту інформації доказової стійкості Мак-Еліса, вперше запропоновану в [8].

Нехай X – невироджена $k \times k$ - матриця над $GF(q)$, D – діагональна матриця з ненульовими на діагоналі елементами, P – перестановочна матриця розміру $n \times n$. Перестановочна матриця реалізує перестановку координат вектора у вигляді матричного множення, а саме: елемент p_{ij} матриці P дорівнює 1 тоді і тільки тоді, коли координата з номером *i* переходить за допомогою перестановки у координату з номером j. У решті випадків $p_{ij} = 0$. Отже, матриця P містить у кожному стовпці і в кожному рядку тільки одну одиницю. Добуток матриць $\Lambda = P \cdot D$ задає перестановочну матрицю Λ з ненульовими елементами поля $GF(q)$. Перестановочна матриця Λ (уніпотентна матриця) при перестановці координат вектора зберігає відстань за Хеммінгом, тобто

$$d(a, b) = d(a \cdot \Lambda, b \cdot \Lambda),$$

де $d(a, b)$ – відстань за Хеммінгом між векторами a і b.

Відкритим ключем у кодовій схемі Мак-Еліса є матриця $G_X = X \cdot G \cdot P \cdot D$, секретним (закритим) ключем є матриці X, P, D. Шифрована інформація (кодограма) у схемі Мак-Еліса є вектором довжини *n* і обчислюється за правилом

$$c_X^* = i \cdot G_X + e, \qquad (1)$$

де вектор $c_X = i \cdot G_X$ належить (n, k, d) коду з породжувальною матрицею G_X; i – k- розрядний інформаційний вектор, $i = \|i_0, i_1, ..., i_{k-1}\|$; $e = \|e_0, e_1, ..., e_{n-1}\|$ – секретний (випадковий) вектор помилок ваги $\le t$.

На рис. 1 наведено схему передавання кодограми у схемі Мак-Еліса.

Зловмисникові необхідно декодувати кодограму c_X^* з відомою породжувальною матрицею G_X. Не знаючи матриці X, P і D, зловмисник не може відновити G і скористатися алгоритмом

декодування поліноміальної складності. Декодування випадкового коду великої довжини обчислювально недоступно (експоненціальна складність при кореляційному декодуванні).

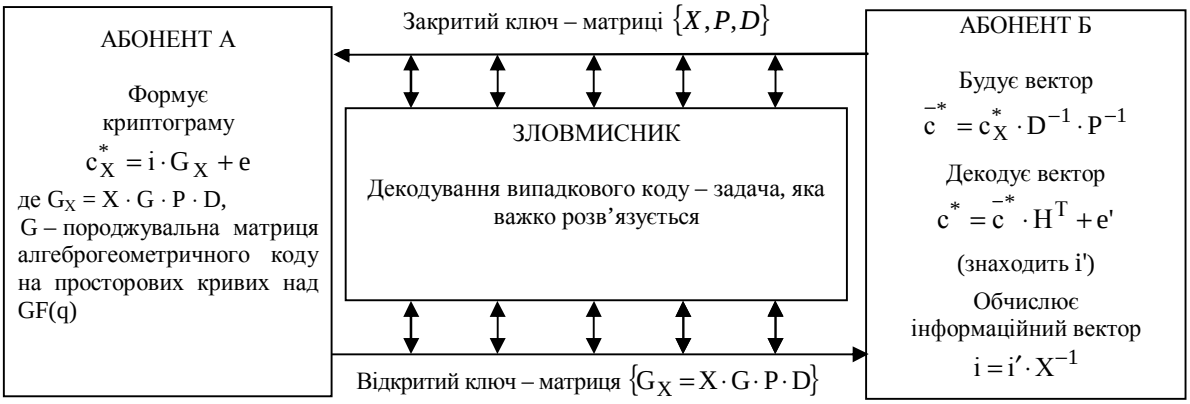

Рис. 1. Схема передавання кодограми в схемі Мак-Еліса

Для уповноваженого користувача (що знає секретний ключ) декодування кодограми – поліноміальне вирішуване завдання. Справді, легітимний користувач, отримавши вектор c_X^*, будує вектор

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \quad (2)$$

Уніпотентна матриця $\Lambda = P \cdot D$ зберігає вагу за Хеммінгом вектора e. Практично це означає, що вектор $\bar{c}^*$ є кодовим словом коду з породжувальною матрицею G, спотворений не більше ніж у t розрядах. Далі уповноважений користувач, користуючись алгоритмом поліноміальної складності, декодує вектор

$$c^* = \bar{c}^* \cdot H^T + e', \quad (3)$$

тобто знаходить i'. Потім обчислює k - розрядний інформаційний вектор

$$i = i' \cdot X^{-1}. \quad (4)$$

Алгеброгеометричні коди на просторових кривих. Зафіксуємо гладку проективну алгебраїчну криву X у проективному просторі P^3 над полем $GF(q)$ як сукупність рішень двох однорідних алгебраїчних незвідних рівнянь від 4-х змінних з коефіцієнтами з $GF(q)$

$$\begin{cases} f_1(x_0, x_1, x_2, x_3) = 0 \\ f_2(x_0, x_1, x_2, x_3) = 0 \end{cases}. \quad (5)$$

Нехай $p_0(x_0, x_1, x_2, x_3)$, $p_1(x_0, x_1, x_2, x_3)$, …, $p_{N-1}(x_0, x_1, x_2, x_3)$ – N сумісних рішень системи рівнянь (5) – точок просторової кривої X. Зафіксуємо дивізор D кривої X і множину раціональних функцій, що асоціюються з дивізором D, тобто множина, яка складається з нуля і функцій $f \neq 0$, для яких $(f) + D \geq 0$. Це еквівалентно набору генераторних функцій

$$F_0(x_0, x_1, x_2, x_3), F_1(x_0, x_1, x_2, x_3), F_2(x_0, x_1, x_2, x_3), \ldots, F_m(x_0, x_1, x_2, x_3), \quad (6)$$

де $F_0, F_1, \ldots, F_m$ – форми однакового ступеня і $F_0(x_0, x_1, x_2, x_3) \neq 0$.

Інакше кажучи, $\varphi(x) = (F_0(x), F_1(x), \ldots, F_m(x))$, як точка в P^m.

Нехай α – ступінь класу дивізорів, $\alpha > g - 1$, тоді відображення $\varphi: X \to P^m$ задає породжувальну матрицю G

$$G = \begin{Vmatrix} F_0(p_0(x_0, x_1, x_2, x_3)) & F_0(p_1(x_0, x_1, x_2, x_3)) & \ldots & F_0(p_{n-1}(x_0, x_1, x_2, x_3)) \\ F_1(p_0(x_0, x_1, x_2, x_3)) & F_1(p_1(x_0, x_1, x_2, x_3)) & \ldots & F_1(p_{n-1}(x_0, x_1, x_2, x_3)) \\ \ldots & \ldots & \ldots & \ldots \\ F_m(p_0(x_0, x_1, x_2, x_3)) & F_m(p_1(x_0, x_1, x_2, x_3)) & \ldots & F_N(p_{n-1}(x_0, x_1, x_2, x_3)) \end{Vmatrix} \quad (7)$$

алгеброгеометричного коду з конструктивними характеристиками $(n \leq N, k \geq \alpha - g + 1, d \geq n - \alpha)$.

Для формування кодового слова $(c_0, c_1, ...c_{n-1})$ алгеброгеометричного коду на просторових кривих, заданого через породжувальну матрицю, достатньо помножити інформаційний вектор $(i_0, i_1, ..., i_{k-1})$ на матрицю (7), тобто для всіх $j = 0,..., n-1$ виконати таке перетворення

$$c_j = \sum_{i=0}^{m-1} i_i F_i\left(p_j(x_0, x_1, x_2, x_3)\right), \quad j = 0,..., n-1 \tag{8}$$

Нехай $\alpha > 2g-2$, тоді відображення $\varphi: X \to P^{m-1}$ задає перевірочну матрицю H

$$H = \begin{Vmatrix} F_0(p_0(x_0, x_1, x_2, x_3)) & F_0(p_1(x_0, x_1, x_2, x_3)) & ... & F_0(p_{n-1}(x_0, x_1, x_2, x_3)) \\ F_1(p_0(x_0, x_1, x_2, x_3)) & F_1(p_1(x_0, x_1, x_2, x_3)) & ... & F_1(p_{n-1}(x_0, x_1, x_2, x_3)) \\ ... & ... & ... & ... \\ F_m(p_0(x_0, x_1, x_2, x_3)) & F_m(p_1(x_0, x_1, x_2, x_3)) & ... & F_N(p_{n-1}(x_0, x_1, x_2, x_3)) \end{Vmatrix} \tag{9}$$

алгеброгеометричного коду з конструктивними характеристиками $(n \le N, k \ge n-\alpha+g-1, d \ge \alpha-2g+2)$.

Добуток прийнятого з помилками кодового слова $c^* = \|c_0 + e_0, c_1 + e_1, ..., c_{n-1} + e_{n-1}\|$ на перевірочну матрицю (9)

$$\left\|c_0^*, c_1^*, ..., c_{n-1}^*\right\| \cdot \begin{Vmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_r(P_0) & F_r(P_1) & ... & F_r(P_{n-1}) \end{Vmatrix}^T \tag{10}$$

дає значення синдромного вектора

$$S = \|S_0, S_1, ..., S_{r-1}\|. \tag{11}$$

Значення синдромного вектора залежить тільки від вектора помилок *e* і не залежить від значення кодового слова *c*

$$S = c^* \cdot H^T = c \cdot H^T + e \cdot H^T = e \cdot H^T, \tag{12}$$

де $c \cdot H^T = 0$.

Розкриємо вираз (10) та з урахуванням (12) подамо елементи синдромного вектора, отримаємо

$$\begin{cases} S_0 = \sum_{i=0}^{n-1} e_i \cdot F_0(P_i); \\ S_1 = \sum_{i=0}^{n-1} e_i \cdot F_1(P_i); \\ \quad ... \\ S_{r-1} = \sum_{i=0}^{n-1} e_i \cdot F_{r-1}(P_i). \end{cases} \tag{13}$$

Задача декодування кодового слова $c^* = \left\|c_0^*, c_1^*, ..., c_{n-1}^*\right\|$ алгеброгеометричного (n, k, d) коду над GF(q) полягає у знаходженні кодового слова *c* і/чи (що еквівалентно) вектора помилок e за відомим вектором c^* і обчисленим за допомогою перевірочної матриці виду (9) елементом синдромного вектора (13).

Для однозначного знаходження вектора помилок скористуємось штучним прийомом, який полягає у введені многочлена локаторів помилок (МЛП) [15, 16]

$$\Lambda(x, y, z) = x^{u-2} + a_{t-3,1,0} \cdot x^{u-3} \cdot y + ... + a_{1,0,0} \cdot x + a_{0,1,0} \cdot y + a_{0,0,1} \cdot z + a_{0,0,0}, \tag{14}$$

рішеннями якого є локатори – такі набори точок (X_ξ, Y_ξ, Z_ξ), які обертають у нуль многочлен (14). МЛП (14) однозначно задає розташування помилок у векторі $e = \|e_0, e_1, ..., e_{n-1}\|$. Знаходження коефіцієнтів a_{i_x, i_y, i_z} МЛП $\Lambda(x, y, z)$ дає змогу однозначно вказати розташування виниклих при

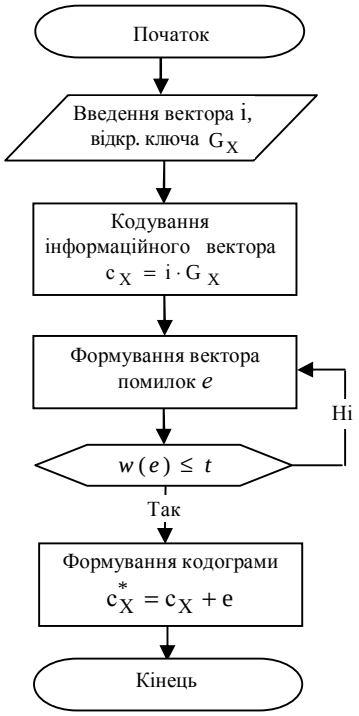

Рис. 2. Схема алгоритму формування кодограми у кодовій схемі захисту інформації Мак-Еліса з АГК на просторових кривих

передачі кодового слова помилок, наприклад, шляхом почергової підстановки всіх наборів (X_j, Y_j, Z_j), j = 0,…, n-1 до многочлена $\Lambda(x, y, z)$ і перевірці його рівності нулю (процедура Ченя).

Дослідження складності реалізації алгоритмів формування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих. Відповідно до основних положень теорії складності час, який затрачується як функція розміру задачі, називається часовою складністю цього алгоритму [5]. Поведінку цієї складності при збільшенні розміру задачі називають асимптотичною часовою складністю алгоритму. Аналогічно визначається ємнісна та асимптотична ємнісна складність алгоритму.

Проведемо оцінку часової та ємнісної складності алгоритмів формування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих та дослідження їх асимптотичної часової і асимптотичної ємнісної складності. Позначимо символом S_E – ємнісну складність алгоритму, тобто кількість необхідних для роботи алгоритму чарунок пам'яті як функцію розміру задачі, і символом S_B – часову складність алгоритму, тобто кількість необхідних для роботи алгоритму елементарних операцій як функцію розміру задачі. На рис. 2. наведено схему алгоритму формування кодограми у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих. Для алгоритму кодування через породжувальну матрицю (7), при відомих (завчасно сформованих) елементів матриці $\left\|F_j(p_i(x_0, x_1, x_2, x_3))\right\|_{n,k}$ необхідно виконати $k \times n$ операцій додавання і добутку. Отже, при затратах $S_E = k \cdot n$ чарунок пам'яті для роботи алгоритму необхідно виконати $S_B = k \cdot n$ елементарних операцій.

Формально ємнісна і часова складності алгоритму кодування через породжувальну матрицю запишеться як асимптотична (в межі при збільшенні розміру задачі) функція $O(r \times n)$.

Для реалізації розглянутих алгоритмів без значних затрат елементів пам'яті формування кодових слів необхідно реалізовувати за допомогою послідовного обчислення значень генераторних функцій у точках просторової кривої. Основною обчислювальною операцією в цьому випадку є знаходження значення генераторної функції $F_j(p_i(x_0, x_1, x_2, x_3))$. Для обчислення $F_j(p_i(x_0, x_1, x_2, x_3))$ потрібні в загальному випадку чотири операції піднесення до степеня і три операції множення. При виконанні аналогічних операцій над однорідними координатами точок кривої потрібно реалізовувати три операції піднесення в степінь і дві операції множення. Якщо прийняти рівними обчислювальну складність операцій множення і піднесення до степеня, маємо $S_E = 3 \cdot n$ чарунок пам'яті для зберігання точок кривої (трьох значень в однорідних координатах для кожної точки) і $S_B = 5 \cdot k \cdot n$ операцій при кодуванні через породжувальну матрицю.

Для кодів над GF(2^m) необхідна організація $S_E = 3 \cdot n \cdot m$ двійкових чарунок пам'яті і $S_B = 5 \cdot k \cdot n \cdot m$ операцій при кодуванні через породжувальну матрицю. Останнім етапом формування кодограми в кодовій схемі захисту інформації Мак-Еліса є сумування кодового слова c_X з вектором помилок e. Відповідно складність усього алгоритму становитиме $((k+1) \cdot n \cdot m)$.

Формально асимптотична ємнісна складність оцінюється як

$$O(n \cdot m), \qquad (15)$$

асимптотична часова складність як

$$O(k \cdot n \cdot m). \qquad (16)$$

Отримана оцінка складності реалізації алгоритмів кодування алгеброгеометричними кодами на просторових кривих показала, що формування кодових слів реалізується з використанням елементарних арифметичних операцій над елементами кінцевого поля і може бути виконано алгоритмами поліноміальної складності від параметрів коду.

Дослідження складності реалізації алгоритмів декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих. Проведемо оцінювання часової та ємнісної складності алгоритмів декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих та дослідження її асимптотичної часової і асимптотичної ємнісної складності.

Аналіз наведеної схеми алгоритму декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих (рис. 3) показує, що для реалізації декодерів алгеброгеометричних кодів на просторових кривих необхідно організувати зберігання параметрів генераторних функцій і точок просторової кривої.

Для зберігання параметрів однієї генераторної функції загального виду (6)

$$F_{i_x,i_y,i_z}(X_j, Y_j, Z_j) = X_j^{i_x} \cdot Y_j^{i_y} \cdot Z_j^{i_z}$$

необхідно організувати 3 чарунки пам'яті, які дадуть змогу зберігати 3 елементи з GF(q). Всього для зберігання параметрів генераторних функцій алгеброгеометричного (n, k, d) коду на просторовій кривій потрібно 3·(n - k) чарунок пам'яті.

Для зберігання однієї точки просторової кривої загального виду (X_j, Y_j, Z_j) необхідно організувати 3 чарунки пам'яті, які дадуть змогу зберігати 3 елементи з GF(q). Разом для зберігання усіх точок просторової кривої алгеброгеометричного (n, k, d) коду потрібно 3·n чарунок пам'яті.

Отже, для реалізації декодерів алгеброгеометричних (n, k, d) кодів над GF(q), заданих на просторових кривих, потрібна організація 6·n - 3·k чарунок пам'яті, які дадуть змогу зберігати 3 елементи з GF(q). Для кодів над GF(2^m) потрібна організація $S_E = 6 \cdot n \cdot m - 3 \cdot k \cdot m$ двійкових чарунок пам'яті.

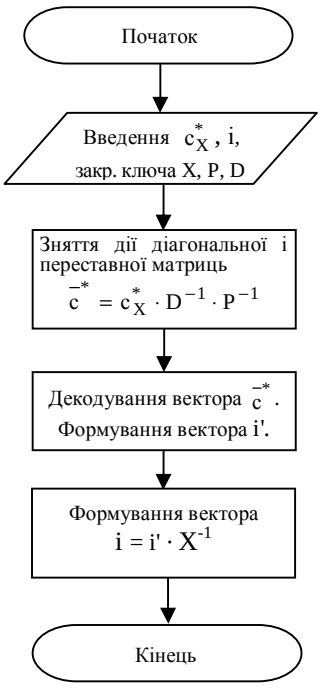

Рис. 3. Схема алгоритму декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з АГК на просторових кривих

Оцінимо часову складність реалізації. Аналіз структурної схеми декодування (рис. 3) показує, що для реалізації декодерів алгеброгеометричнх кодів на просторових кривих необхідно організувати обчислення елементів породжувальної матриці, синдромної послідовності, розв'язання систем рівнянь (13) і (14), обчислення локаторів помилок, а також організувати виправлення помилок у кодовій послідовності.

Для обчислення одного елемента породжувальної матриці необхідно виконати три операції піднесення до степеня і два добутки над GF(q). При обчисленні синдромної послідовності кожний елемент породжувальної матриці помножують на відповідний елемент кодової послідовності. Отже, для обчислення елементів синдромної послідовності з урахуванням операції на формування елементів породжувальної матриці необхідно виконати 3·(n - k) операції піднесення до степеня, 3·(n - k) множення і n - k - 1 операцій додавання над GF(q).

Розв'язуючи систему рівнянь (14), потрібно v^2 операцій множення і додавання над GF(q), де v – число невідомих. Проведемо оцінку v. Число невідомих v в системі (14) визначається числом одночленів від чотирьох змінних степеня $(u-2)$, де u – число помилок. Оскільки $u \le t$ – число невідомих v не вище кількості одночленів степеня $(t-2)$. У загальному

випадку число одночленів степеня a в P^n задається значенням біноміального коефіцієнта C^n_{a+n}. Отже, число невідомих v в системі (14) обмежено зверху виразом

$$v \le C^3_{(t-2)+3} = C^3_{t+1} = \frac{(t+1)!}{3!(t-2)!} = \frac{(t+1)\cdot(t)\cdot(t-1)}{2\cdot 3} = \frac{t^3-t}{6}.$$

Тоді для розв'язання системи рівнянь (14) потрібно не більше ніж

$$\left(\frac{t^3-t}{6}\right)^2 = \frac{t^6-2\cdot t^4+t^2}{36}$$

операцій множення і додавання над GF(q).

Для розв'язання системи рівнянь (13) потрібно u^2 операцій множення і додавання над GF(q), де $u \le t$. Оцінка зверху часової складності реалізації цього етапу декодування дає не більше t^2 операцій множення і додавання над GF(q).

Для знаходження локаторів помилок необхідно підставити всі проективні точки просторової кривої у многочлен локаторів помилок і перевірити на рівність його нулю (процедура Ченя) [3]. Для цього в загальному випадку необхідно виконати 3·v·n операцій піднесення до степеня, множення і v·n операцій додавання над GF(q). З урахуванням зроблених вище міркувань обчислювальна складність цього етапу декодування становитиме не більше $\frac{t^3-t}{2}n$ операцій піднесення до степеня і множення над GF(q) і $\frac{t^3-t}{6}n$ операцій додавання над GF(q).

Для виправлення помилок у кодовій послідовності необхідно виконати операцію віднімання (для полів характеристики два – операцію додавання) кодового слова з помилками і вектора помилок. Для цього необхідно виконати n операцій віднімання (додавання) над GF(q).

Отже, як показали проведені дослідження, для реалізації алгебраїчного декодування кодів на просторових кривих необхідно виконати

$$3\cdot(n-k)+\frac{t^3-t}{2}n$$

операцій піднесення до степеня

$$3\cdot(n-k)+\frac{t^6-2\cdot t^4+t^2}{36}+t^2+\frac{t^3-t}{2}n$$

операцій множення і

$$(n-k-1)+\frac{t^6-2\cdot t^4+t^2}{36}+t^2+\frac{t^3-t}{6}n \qquad (17)$$

операцій додавання над *GF(q)*.

Крім того, для відновлення кодограми (зняття матриць маскування) необхідно помножити кодограму на матриці D^{-1}, P^{-1}, X^{-1}. Складність цих кроків відповідно становить

$$2\cdot n^2+k^2 \qquad (18)$$

операцій множення і операцій додавання над GF(q).

Загальна часова складність декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих з урахуванням (17) і (18) становить

$$S_B = (2\cdot n^2+k^2+(n-k-1)+\frac{t^6-2\cdot t^4+t^2}{36}+t^2+\frac{t^3-t}{6}n)$$

і задається поліноміальною функцією від довжини коду і його виправляючою здібністю.

Тоді асимптотична часова складність дорівнюватиме

$$O(n^2+k^2+t^6). \qquad (19)$$

Висновки

Отже, для інтегрованого забезпечення конфіденційності та достовірності передавання повідомлень у ТССП, актуальним питанням є використання кодових схем захисту інформації доказової стійкості з використанням алгеброгеометричних кодів на просторових кривих.

Розглянуто питання побудови кодової схеми захисту інформації Мак-Еліса з використанням алгеброгеометричних кодів на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних. Досліджено складність реалізації алгоритмів формування та декодування кодограм у кодовій схемі захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих.

У результаті проведених досліджень формування кодограми показало, що часова і ємнісна складність реалізації алгоритмів, формування кодових слів реалізуються з використанням елементарних арифметичних операцій над елементами кінцевого поля і можуть бути виконані алгоритмами поліноміальної складності від параметрів коду. Аналіз процедур декодування кодограм показав, що для сучасної обчислювальної техніки реалізація декодерів алгеброгеометричних кодів з $n = (10^2 \div 10^4)$ не є складною. Водночас реалізація декодерів доцільна лише для виправляючої здатності $t = (10 \div 10^2)$. Реалізація декодерів алгеброгеометричних кодів на просторових кривих з $t > 10^2$ на сучасній обчислювальній техніці значно утруднена і, очевидно, недоцільна.

Подальшим напрямком досліджень є дослідження стійкості до злому кодової схеми захисту інформації Мак-Еліса з алгеброгеометричними кодами на просторових кривих.

1. Інформаційний огляд "Техніка та озброєння. Розроблення, модернізація, випробування та прийняття на озброєння". Органи управління РВіА: стан і перспективи розвитку. – Суми: НЦ БЗ РВіА, 2006. – С. 5–7. 2. Сігуткін Є.Г. Перспективи розвитку бойового застосування і підвищення ефективності управління ракетними військами та артилерією Збройних Сил України // Артиллерийское и стрелковое вооружение: Международный научн.-техн. сб. – К.: НТЦ АСВ, 2000. – Вып. 2. – С. 26–31. 3. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с. 4. Злотник Б. М. Помехоустойчивые коды в системах святи / Б. М. Злотник. – М.: Радио и связь, 1989. – 232 с. 5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с. 6. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с. 7. Онанченко Е.Л. Исследование методов защиты информации, основанных на использовании алгебраических блоковых кодов / Е.Л. Онанченко, А.А. Кузнецов, В.Н.Лисенко, В.И. Грабчак, Р.В. Королев // Системи обробки інформації. – Харків: ХУ ПС. – 2007. – Вип. 7 (65). – С. 53 – 59. 8. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114–116. 9. Niederreiter H.. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theorty. – 1986. –V.15. – P. 19–34. 10. Сидельников В.М. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона / В.М. Сидельников, С.О. Шестаков // Дискретная математика. – 1992.– Т.4.№3. – С.57–63. 11. Грабчак В.І. Кодові схеми захисту інформації доказової стійкості на просторових кривих / В.І. Грабчак, З.М. Грабчак, І.В. Пасько, П.Є. Трофіменко // Технічні вісті. – Львів: НУ "ЛП". – 2010. – Вип. 1(31), 2(32). – С.51 – 58. 12. Грабчак В.И. Алгебраическое кодирование алгеброгеометрическими кодами на пространственных кривых / В.И. Грабчак, И.В. Пасько, Р.В. Королев, И.Е. Кужель // Системи обробки інформації. – Харків: ХУПС. – 2007. – Вип. 8 (66). – С.134–139. 13. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования / А.А. Кузнецов // Всеукр. меж вед. науч.-техн. сб. – Харків: ХТУРЭ, 2003. – Вып.134. – С. 218–222. 14. Кузнецов А.А. Исследование помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых. / А.А. Кузнецов, В.И. Грабчак, И.В. Пасько // Системи управління, навігації та зв'язку. – К: ЦНДІНіУ. – 2007. – Вип. 3. – С.82–85.