Інформаційна безпека

УДК 621.391

В.І. Грабчак[1], І.В. Пасько[2]

[1] *Академія сухопутних військ, Львів*
[2] *Науковий центр бойового застосування ракетних військ і артилерії, Суми*

СХЕМИ ЗАХИСТУ ІНФОРМАЦІЇ МАК-ЕЛЛІСА З АЛГЕБРОГЕОМЕТРИЧНИМИ КОДАМИ НА ПРОСТОРОВИХ КРИВИХ

У статті досліджуються питання побудови кодових схем захисту інформації доказової стійкості Мак-Елліса з використанням алгеброгеометричних кодів на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних, застосування яких дозволить інтегровано забезпечити достовірність і конфіденційність інформації у телекомунікаційних системах. Наведений приклад їх практичної реалізації.

Ключові слова: *кодові схеми захисту інформації, схема Мак-Елліса, алгеброгеометричні коди на просторових кривих.*

Вступ

Перспективним напрямом у розвитку механізмів інтегрованого забезпечення достовірності і конфіденційності передачі повідомлень у системах передачі даних є кодові схеми захисту інформації доказової стійкості [1 – 4]. Це криптографічні системи, побудова яких основана на маскуванні блокових алгебраїчних кодів зі швидкими алгоритмами декодування під випадковий код і зведенні задачі зламу криптографічної системи до теоретико-складної задачі декодування випадкового коду [5 – 7]. Їх практичне використання дозволяє реалізувати в одному пристрої методи канального кодування і спеціального перетворення даних.

На сьогоднішній день розглянуті приклади побудови кодових схем захисту інформації доказової стійкості Мак-Елліса та Нідеррайтера на основі кодів Боуза-Чоудхурі-Хоквінгема (БЧХ) і кодів Ріда-Соломона (РС) (підклас недвійкових кодів БЧХ). У [1] запропонований ефективний метод зламу схеми Мак-Елліса з кодом РС. Там же автором висувається припущення про потенційну вразливість схем, які побудовані на узагальнених кодах БЧХ. Крім того, процедури зламу схеми Мак-Елліса можуть бути легко трансформовані на схеми Нідеррайтера. Стійкість кодових схем захисту інформації, побудованих на кодах РС і кодах БЧХ, вважається недостатньою.

Одним із перспективних напрямів розвитку кодових схем захисту інформації доказової стійкості, спрямованих на підвищення стійкості, є використання кодів, побудованих по алгебраїчних кривих (алгеброгеометричних кодів – АГК), застосування яких дозволить отримати додатковий параметр маскування коду – вид алгебраїчної кривої [8, 9], на основі якої будується перевірочна і породжувальна матриця коду. Крім того, в роботах [10, 11] показано, що використання АГК для передачі повідомлень по дискретних каналах зв'язку дозволяє отримати значний енергетичний виграш від кодування.

Водночас проведені дослідження АГК для плоских алгебраїчних кривих, заданих в проективному просторі P^2 однорідним незвідним рівнянням від трьох змінних. Перспективним напрямом подальших досліджень для формування кодових схем захисту інформації доказової стійкості є використання АГК на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних [12 – 14]. Застосування кодів, побудованих по просторових кривих, для формування кодової схеми дозволить отримати ще один додатковий параметр маскування коду – вид другої алгебраїчної кривої та підвищити енергетичний виграш від кодування [13].

Метою статті є побудова кодових схем захисту інформації доказової стійкості Мак-Елліса з використанням АГК на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних, розробка практичних процедур їх формування та декодування.

Основна частина

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):

$$\begin{cases} f_1(x_0, x_1, x_2, x_3) = 0, \\ f_2(x_0, x_1, x_2, x_3) = 0. \end{cases} \quad (1)$$

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 (1) – точок просторової кривої X. Зафіксуємо дивізор D кривої X і множину раціональних функцій, що асоціюються з дивізором D, тобто множина, що складається з нуля і функцій $f \neq 0$, для яких $(f)+D \geq 0$. Це еквівалентно набору генераторних функцій

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

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

$$G = \begin{Vmatrix} F_0(p_0(x_0,x_1,x_2,x_3)) & \ldots & F_0(p_{n-1}(x_0,x_1,x_2,x_3)) \\ F_1(p_0(x_0,x_1,x_2,x_3)) & \ldots & F_1(p_{n-1}(x_0,x_1,x_2,x_3)) \\ & \ldots & \\ F_N(p_0(x_0,x_1,x_2,x_3)) & \ldots & F_N(p_{n-1}(x_0,x_1,x_2,x_3)) \end{Vmatrix} \quad (2)$$

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

Визначення 1. АГК на просторовій кривій X над $GF(q)$, побудований через породжувальну матрицю G – це лінійний код, всі кодові слова $(c_0,c_1,\ldots c_{n-1})$ якого задаються рівністю:

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

Для формування кодового слова $(c_0,c_1,\ldots c_{n-1})$ АГК на просторових кривих, заданого через породжувальну матрицю досить помножити інформаційний вектор $(i_0,i_1,\ldots,i_{k-1})$ на матрицю (2), тобто для всіх $j=0,\ldots,n-1$ виконати наступне перетворення

$$c_j = \sum_{i=0}^{m-1} i_i F_i(p_j(x_0,x_1,x_2,x_3)). \quad (3)$$

Нехай $\alpha > 2g-2$, тоді відображення

$$\varphi: X \to P^{m-1}$$

задає перевірочну матрицю

$$H = \begin{Vmatrix} F_0(p_0(x_0,x_1,x_2,x_3)) & \ldots & F_0(p_{n-1}(x_0,x_1,x_2,x_3)) \\ F_1(p_0(x_0,x_1,x_2,x_3)) & \ldots & F_1(p_{n-1}(x_0,x_1,x_2,x_3)) \\ & \ldots & \\ F_N(p_0(x_0,x_1,x_2,x_3)) & \ldots & F_N(p_{n-1}(x_0,x_1,x_2,x_3)) \end{Vmatrix} \quad (4)$$

АГК з конструктивними характеристиками $(n \leq N,\ k \geq n-\alpha+g-1,\ d \geq \alpha-2g+2)$.

Визначення 2. Добуток прийнятого з помилками кодового слова $c^* = \|c_0+e_0, c_1+e_1, \ldots, c_{n-1}+e_{n-1}\|$ на перевірочну матрицю (4)

$$\|c_0^*, c_1^*, \ldots, c_{n-1}^*\| \cdot \begin{Vmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_r(P_0) & F_r(P_1) & \ldots & F_r(P_{n-1}) \end{Vmatrix}^T \quad (5)$$

дає значення синдромного вектора

$$S = \|S_0, S_1, \ldots, S_{r-1}\|. \quad (6)$$

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

$$S = c^* \cdot H^T = c \cdot H^T + e \cdot H^T = e \cdot H^T, \quad (7)$$

де $c \cdot H^T = 0$.

Розкриємо скобки у виразі (5) та з урахуванням (7) виразимо елементи синдромного вектора, отримаємо

$$\begin{cases} S_0 = \sum_{i=0}^{n-1} e_i \cdot F_0(P_i); \\ S_1 = \sum_{i=0}^{n-1} e_i \cdot F_1(P_i); \\ \ldots \\ S_{r-1} = \sum_{i=0}^{n-1} e_i \cdot F_{r-1}(P_i). \end{cases} \quad (8)$$

Задача декодування кодового слова $c^* = \|c_0^*, c_1^*, \ldots, c_{n-1}^*\|$ АГК 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 (4) елементам синдромного вектора (8).

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

$$\Lambda(x,y,z) = x^{u-2} + a_{t-3,l,0} \cdot x^{u-3} \cdot y + \ldots + a_{1,0,0} \cdot x + a_{0,1,0} \cdot y + a_{0,0,1} \cdot z + a_{0,0,0}, \quad (9)$$

рішеннями якого є локатори – такі набори точок (X_ξ, Y_ξ, Z_ξ), які обертають у нуль многочлен (9). МЛП (9) однозначно задає розташування помилок у векторі $e = \|e_0, e_1, \ldots, e_{n-1}\|$. Знаходження коефіцієнтів a_{i_x,i_y,i_z} МЛП $\Lambda(x,y,z)$ дозволяє однозначно вказати розташування виниклих при передачі кодового слова помилок, наприклад, шляхом почергової підстановки всіх наборів (X_j, Y_j, Z_j), $j = 0,\ldots, n-1$ до многочлена $\Lambda(x,y,z)$ і перевірці його рівності нулю.

Кодові схеми захисту інформації доказової стійкості. Розглянемо кодову схему захисту інформації доказової стійкості Мак-Елліса, вперше запропоновану в [5].

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 $p_{ij} = 0$. Таким чином, 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 по Хеммінгу, тобто $d(a,b) = d(a \cdot \Lambda, b \cdot \Lambda)$, де $d(a,b)$ – відстань по Хеммінгу між векторами a і b.

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

$$c_X^* = i \cdot G_X + e, \qquad (10)$$

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 представлена схема передачі кодограми в схемі Мак-Елліса.

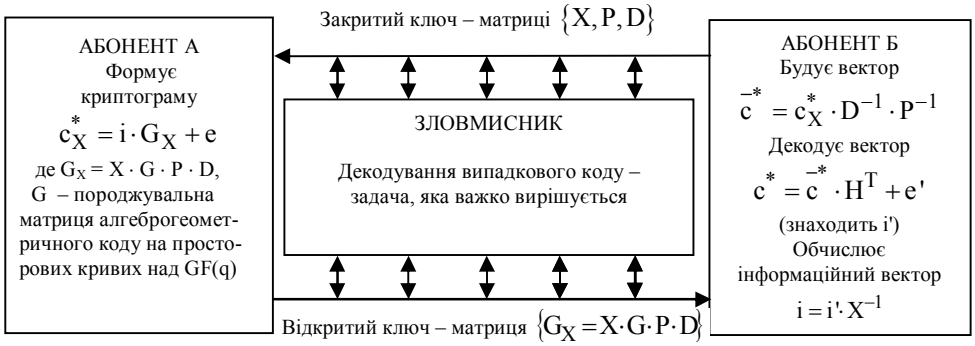


Рис. 1. Схема передачі кодограми в схемі Мак-Елліса

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).

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

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \qquad (11)$$

Уніпотентна матриця $\Lambda = P \cdot D$ зберігає вагу по Хеммінгу 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

$$c^* = \bar{c}^* \cdot H^T + e', \qquad (12)$$

тобто знаходить i'. Потім обчислює k-розрядний інформаційний вектор $i = i' \cdot X^{-1}$.

Слід зазначити, що побудова кодових схем захисту інформації базується на маскуванні завадостійкого (n, k, d) блокового коду зі швидким алгоритмом декодування під випадковий код. При цьому в кодове слово (n, k, d) блокового коду вноситься випадковий вектор помилок e, вага якого менше або рівна виправляючій здатності коду

$$w(e) \le t, \qquad (13)$$

де $t = \lfloor d - 1/2 \rfloor$.

Позначимо частку ваги вектора помилок вектора e, що доводиться на штучне внесення кодовою Мак-Елліса, символом ρ:

$$\rho = w(e)/t. \qquad (14)$$

Тоді потенційна стійкість кодової схеми Мак-Елліса визначатиметься величиною $\rho \cdot t$, а завадостійкість кодограм, що передаються, визначатиметься величиною $(1-\rho) \cdot t$. Варіюючи часткою виправляючої здатності АГК, що доводиться на штучне внесення помилок – ρ, можна інтегровано (одним

прийомом) забезпечити конфіденційність і достовірність передачі повідомлень. Причому за умови:

$\rho = 0$ – режим забезпечення достовірності (завадостійкого кодування);

$\rho = 1$ – режим забезпечення конфіденційності;

$0 > \rho > 1$ – режим інтегрованого забезпечення конфіденційності і достовірності передачі повідомлень.

Приклад формування кодограми в кодовій схемі захисту інформації Мак-Елліса. Зафіксуємо два алгебраїчні рівняння $xy^2 + x^2z + yz^2 = 0$ та $yz^2 + y^2v + yv^2 = 0$ над полем $GF(2^2)$, множина сукупних рішень яких задає просторову криву. Після підстановки елементів поля $GF(2^2)$ до рівняння отримаємо їх рішення (табл. 1 і 2).

Таблиця 1

Рішення рівняння $xy^2 + x^2z + yz^2 = 0$ над полем GF (2^2)

x	y	z	v	x	y	z	v	x	y	z	v	x	y	z	v
1	0	0	0	1	0	0	1	2	2	1	1	0	0	3	1
0	1	0	0	2	0	0	1	1	3	1	1	1	1	3	1
0	0	1	0	3	0	0	1	3	3	1	1	3	1	3	1
2	1	1	0	0	1	0	1	0	0	2	1	2	2	3	1
3	1	1	0	0	2	0	1	1	1	2	1	3	2	3	1
1	2	1	0	0	3	0	1	2	1	2	1	1	3	3	1
2	2	1	0	0	0	1	1	1	2	2	1	2	3	3	1
1	3	1	0	2	1	1	1	3	2	2	1				
3	3	1	0	3	1	1	1	2	3	2	1				
0	0	0	1	1	2	1	1	3	3	2	1				

Примітка: тут і далі 1, 2, 3 відповідають примітивним елементам поля $GF(2^2)$ – $\alpha^0, \alpha^1, \alpha^2$.

Таблиця 2

Рішення рівняння $yz^2 + y^2v + yv^2 = 0$ над полем GF (2^2)

x	y	z	v	x	y	z	v	x	y	z	v	x	y	z	v
1	0	0	0	1	0	0	1	3	3	1	1	1	1	3	1
0	1	0	0	2	0	0	1	0	1	2	1	2	1	3	1
1	1	0	0	3	0	0	1	1	1	2	1	3	1	3	1
2	1	0	0	0	2	1	1	2	1	2	1	0	3	3	1
3	1	0	0	1	2	1	1	3	1	2	1	1	3	3	1
0	0	1	0	2	2	1	1	0	2	2	1	2	3	3	1
1	0	1	0	3	2	1	1	1	2	2	1	3	3	3	1
2	0	1	0	0	3	1	1	2	2	2	1				
3	0	1	0	1	3	1	1	3	2	2	1				
0	0	0	1	2	3	1	1	0	1	3	1				

Сумісні рішення рівнянь $xy^2 + x^2z + yz^2 = 0$ та $yz^2 + y^2v + yv^2 = 0$ надані в табл. 3.

На множині точок $\{P_0, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{11}\}$ побудуємо алгеброгеометричний код.

Таблиця 3

Сумісні рішення рівнянь $xy^2+x^2z+yz^2=0$ та $yz^2+y^2v+yv^2=0$ над полем GF (2^2)

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
x	1	3	2	1	1	1	2	3	1	3	1	2
y	2	3	2	2	3	1	1	2	1	1	3	3
z	2	1	1	1	1	2	2	2	3	3	3	3
v	1	1	1	1	1	1	1	1	1	1	1	1

Зафіксуємо множину генераторних функцій у вигляді одночленів степені deg = 2: { x^2, y^2, z^2, v^2, xy, xz, xv, yz, yv, zv }. Обчислимо значення генераторних функцій у точках кривої і сформуємо перевірочну матрицю коду (табл. 4).

Таблиця 4

Значення генераторних функцій у точках просторової кривої

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
x^2	1	2	3	1	1	1	3	2	1	2	1	3
y^2	3	2	3	3	2	1	1	3	1	1	2	2
z^2	3	1	1	1	1	3	3	3	2	2	2	2
xy	2	2	3	2	3	1	2	1	1	3	3	1
xz	2	3	2	1	1	2	3	1	3	1	3	1
xv	1	2	2	1	1	1	2	3	1	3	1	2
yz	3	3	2	2	3	2	2	3	3	3	2	2
yv	2	3	2	2	3	1	1	2	1	1	3	3
zv	2	1	1	1	1	2	2	2	3	3	3	3

Перевірочна матриця H, побудована по значеннях генераторних функцій у точках просторової кривої (табл. 4), транспонована перевірочна матриця H^T та відповідна породжувальна матриця G мають вигляд

$$H = \begin{Vmatrix} 123111321213 \\ 323321131122 \\ 311113332222 \\ 223231211331 \\ 232112313131 \\ 122111231313 \\ 332232233322 \\ 232231121133 \\ 211112223333 \end{Vmatrix}, \quad H^T = \begin{Vmatrix} 133221322 \\ 221232331 \\ 331322221 \\ 131211221 \\ 121311331 \\ 113121212 \\ 313232212 \\ 233113322 \\ 112131313 \\ 212323313 \\ 122331233 \\ 322112233 \end{Vmatrix},$$

$$G = \begin{Vmatrix} 100320330212 \\ 010332120230 \\ 001310213220 \end{Vmatrix} \qquad (15)$$

та задають (12, 3, 8) код, який виправляє будь-яку конфігурацію з трьох помилок, при чому виконується рівність $G \cdot H^T = 0$.

Відкритим ключем є матриця G_X :

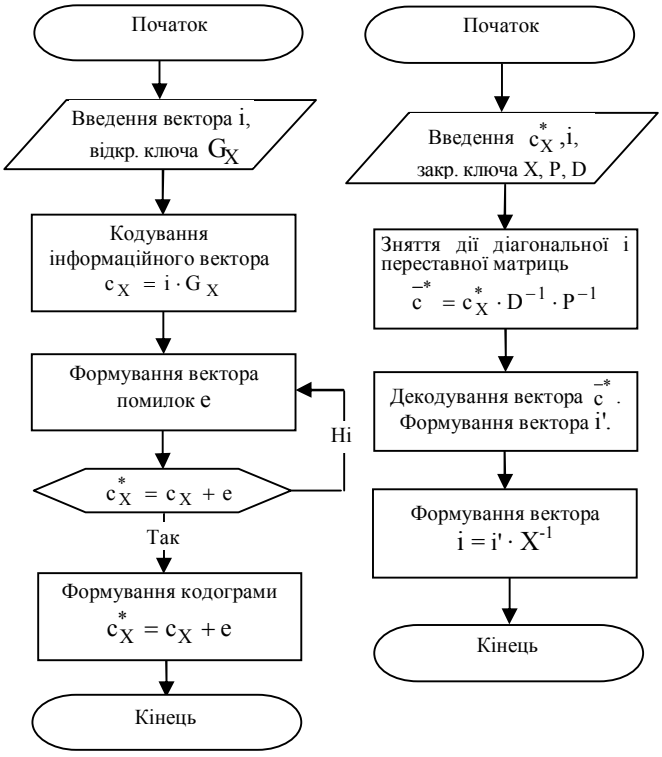
$$G_X = \begin{Vmatrix} 300030131111 \\ 021132100011 \\ 031020310211 \end{Vmatrix}, \qquad (16)$$

де

$$G_X = X \cdot G \cdot P \cdot D,\ X = \begin{Vmatrix} 010 \\ 203 \\ 021 \end{Vmatrix},$$

$$P = \begin{Vmatrix} 000100000000 \\ 000000000100 \\ 001000000000 \\ 000010000000 \\ 100000000000 \\ 000000010000 \\ 000000001000 \\ 000000000001 \\ 010000000000 \\ 000000100000 \\ 000000000010 \\ 000001000000 \end{Vmatrix},\ D = \begin{Vmatrix} 100000000000 \\ 010000000000 \\ 002000000000 \\ 000300000000 \\ 000010000000 \\ 000003000000 \\ 000000300000 \\ 000000020000 \\ 000000001000 \\ 000000000100 \\ 000000000020 \\ 000000000003 \end{Vmatrix}.$$

Алгоритм формування кодограми в кодовій схемі захисту інформації Мак-Елліса надамо у вигляді послідовності наступних кроків (рис. 2, а):



а – формування кодограми

б – декодування кодограми

Рис. 2. Алгоритм функціонування кодової схеми захисту інформації Мак-Елліса з АГК на просторових кривих

1. Введення інформації, яка підлягає кодуванню. Введення відкритого ключа G_X (16).

2. Кодування інформації АГК на просторових кривих. Формування кодового слова c_X. АГК на просторових кривих, який задається матрицею G_X.

3. Формування вектора помилок e (13), вага якого не перевищує $\le t$ – виправляючу здатність АГК на просторових кривих.

4. Формування кодограми $c_X^* = c_X + e$.

Нехай інформаційний вектор $i = \|2,1,3\|$, тоді для формування кодового слова $(c_0, c_1, ...c_{n-1})$ достатньо помножити інформаційний вектор на породжувальну матрицю – $c_X = i \cdot G_X$. Після виконання множення кодове слово запишеться у вигляді $c_X = \|100132122300\|$.

Штучно внесемо помилку в кодове слово для забезпечення потенційної стійкість кодової схеми. Вектор помилок позначимо як $e = (e_0, e_1, ..., e_{n-1}) = \|000010000002\|$. Крім того, уявимо, що при передачі по каналу з помилками кодове слово спотворилося, вектор помилок позначимо як $e = (e_0, e_1, ..., e_{n-1}) = \|003000000000\|$. Загальний вектор помилок буде мати вигляд $e = \|003010000002\|$. Прийняте слово з помилками c_X^*, запишеться як $c_X^* = c_X + e = \|c_0 + e_0, c_1 + e_1, ..., c_{11} + e_{11},\|$ і дорівнює

$$c_X^* = \|100132122300\| \oplus \|003010000002\| = \|103122122302\|.$$

Приклад декодування кодограми в кодовій схемі захисту інформації Мак-Елліса. Для декодування кодограми в кодовій схемі захисту інформації Мак-Елліса необхідно зняти дію діагональної D і перестановочної P матриць. Потім, декодуваши отриманий вектор, необхідно зняти дію матриці X .

Алгоритм декодування кодограми надамо у вигляді послідовності наступних кроків (рис. 2, б):

1. Введення кодограми c_X^*, яка підлягає декодуванню. Введення закритого ключа – матриці X, P, D.

2. Зняття дії діагональної і перестановочної матриць $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$.

3. Декодування вектора $\bar{c}^*$. Формування вектора i'.

4. Зняття дії матриці X: $i = i' \cdot X^{-1}$. Формування інформаційного вектора i.

Знімаємо дію матриць маскування P, D :

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1},$$

де

$$P^{-1} = \begin{Vmatrix} 000010000000 \\ 000000001000 \\ 001000000000 \\ 100000000000 \\ 000100000000 \\ 000000000001 \\ 000000000100 \\ 000001000000 \\ 000000100000 \\ 010000000000 \\ 000000000010 \\ 000000010000 \end{Vmatrix}, \quad D^{-1} = \begin{Vmatrix} 100000000000 \\ 010000000000 \\ 003000000000 \\ 000200000000 \\ 000010000000 \\ 000002000000 \\ 000000200000 \\ 000000030000 \\ 000000001000 \\ 000000000100 \\ 000000000030 \\ 000000000002 \end{Vmatrix}.$$

Отримаємо кодове слово $\bar{c}^{*} = \|232211230203\|$.

Кодове слово помножимо на транспоновану перевірочну матрицю (15) та отримаємо синдромний вектор (6), який дорівнює:

$$s_{2,0,0} = 1;\ s_{0,2,0} = 0;\ s_{0,0,2} = 1;$$

$$s_{1,1,0} = 0;\ s_{0,0,1} = 2;\ s_{1,0,0} = 3;\ s_{0,1,1} = 3;\ s_{0,1,0} = 0;$$

$$s_{1,0,1} = 1. \qquad (17)$$

Побудуємо МЛП (8). Кількість помилок, які може виправити код $t = 3$, МЛП у загальному вигляді отримає вигляд

$$\Lambda(x, y, z) = x + a_{0,1,0} \cdot y + a_{0,0,1} \cdot z + a_{0,0,0}, \quad (18)$$

рішеннями якого є локатори – такі набори точок (X, Y, Z), які обертають у нуль многочлен (18).

Сформуємо систему лінійних рівнянь

$$\begin{cases} s_{2,0,0} + a_{0,1,0} \cdot s_{1,1,0} + a_{0,0,1} \cdot s_{1,0,1} + a_{0,0,0} \cdot s_{1,0,0} = 0; \\ s_{1,1,0} + a_{0,1,0} \cdot s_{0,2,0} + a_{0,0,1} \cdot s_{0,1,1} + a_{0,0,0} \cdot s_{0,1,0} = 0; \\ s_{1,0,1} + a_{0,1,0} \cdot s_{0,1,1} + a_{0,0,1} \cdot s_{0,0,2} + a_{0,0,0} \cdot s_{0,0,1} = 0. \end{cases} \quad (19)$$

Підставляючи значення (17) у (19), та вирішуючи систему, отримаємо

$$\begin{cases} a_{0,1,0} = 3; \\ a_{0,0,0} = 1; \\ a_{0,0,1} = 2. \end{cases} \quad (20)$$

Підставивши знайдені коефіцієнти $a_{0,0,0}, a_{0,0,1}, a_{0,1,0}$ у МЛП (18), отримаємо

$$\Lambda(x, y, z) = x + 3 \cdot y + 2 \cdot z + 1. \quad (21)$$

Скористаємося процедурою Ченя [15, 16]. Підставимо всі точки просторової кривої (табл. 3) у многочлен локаторів помилок (21). Ті пари, які при підстановці обертають його в нуль, локалізують помилки, тобто вказують на їх розташування, маємо:

P_0: $\Lambda(1,2,2) \neq 0$; P_1: $\Lambda(3,3,1) \neq 0$; P_2: $\Lambda(2,2,1) = 0$;

P_3: $\Lambda(1,2,1) \neq 0$; P_4: $\Lambda(1,3,1) = 0$; P_5: $\Lambda(1,1,2) \neq 0$;

P_6: $\Lambda(2,1,2) \neq 0$; P_7: $\Lambda(3,2,2) = 0$; P_8: $\Lambda(1,1,3) \neq 0$;

P_9: $\Lambda(3,1,3) = 0$; P_{10}: $\Lambda(1,3,3) \neq 0$; P_{11}: $\Lambda(2,3,3) = 0$.

Пари $(2,2,1), (1,3,1), (3,2,2), (3,1,3), (2,3,3)$ обертають його в нуль, тобто локалізують помилки, вказуючи, що помилки розташовані у символах $c_2^*, c_4^*, c_7^*, c_9^*, c_{10}^*, c_{11}^*$ кодового слова. Як витікає з отриманих результатів, помилка локалізована у наступних символах $\|00e_2 0e_4 00e_7 0e_9 e_{10} e_{11}\|$.

Отриманий вектор помилок помножимо на транспоновану перевірочну матрицю (15), отримаємо

$$s_{0,0,0} = \sum_{j=0}^{11} e_j;\ s_{1,0,0} = \sum_{j=0}^{11} e_j \cdot X_j;\ s_{0,1,0} = \sum_{j=0}^{11} e_j \cdot Y_j;$$

$$s_{0,0,1} = \sum_{j=0}^{11} e_j \cdot Z_j;\ s_{1,1,0} = \sum_{j=0}^{11} e_j \cdot X_j \cdot Y_j;$$

$$s_{1,0,1} = \sum_{j=0}^{11} e_j \cdot X_j \cdot Z_j;\ s_{0,1,1} = \sum_{j=0}^{11} e_j \cdot Y_j \cdot Z_j;$$

$$s_{2,0,0} = \sum_{j=0}^{11} e_j \cdot X_j^2;\ s_{0,2,0} = \sum_{j=0}^{11} e_j \cdot Y_j^2;$$

$$s_{0,0,2} = \sum_{j=0}^{11} e_j \cdot Z_j^2.$$

Розв'язавши останню систему, одержимо:

$$e_1 = 0;\ e_2 = 3;\ e_4 = 1;\ e_7 = 0;\ e_9 = 0;\ e_{10} = 0;$$

$$e_{11} = 2.$$

Сформуємо вектор помилок $e = \|003010000002\|$.

Відновимо кодове слово *c* за відомою послідовністю $\bar{c}^{*}$ і знайденому вектору помилок

$$c = \bar{c}^{*} - e = (\bar{c}_0^{*} - e_0, \bar{c}_1^{*} - e_1, ..., \bar{c}_{11}^{*} - e_{11})$$

$$\bar{c}^{*} + e = \|233211230203\| \oplus \|003010000002\| =$$

$$= \|23010230201\|.$$

Помилка локалізована та виправлена, задача декодування вирішена.

На останньому кроці обчислимо інформаційний вектор $i = i' \cdot X^{-1}$, який дорівнює

$$\|230\| \cdot \begin{Vmatrix} 332 \\ 100 \\ 201 \end{Vmatrix} = \|213\|.$$

Задача відновлення інформаційного вектора вирішена.

Висновки

Для інтегрованого забезпечення конфіденційності та достовірності передачі повідомлень у телекомунікаційних системах, актуальним питанням є використання кодових схем захисту інформації доказової стійкості з використанням АГК на просторових кривих. У статті розглянуті теоретичні питання побудови кодової схеми захисту інформації Мак-

Елліса з використанням АГК на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних та наведено практичний приклад її реалізації. Застосування кодів, побудованих по просторових кривих, для формування кодової схеми дозволить отримати ще один додатковий параметр маскування коду – вид другої алгебраїчної кривої. Перспективним напрямком подальших досліджень є визначення кількісних показників часової та ємкісної складності запропонованих процедур формування і декодування кодових схем захисту інформації Мак-Елліса з використання АГК на просторових кривих.

Список літератури

1. 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.

2. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ, 2002. – 22 с.

3. 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. – Х.: ХУ ПС, 2007. – Вип. 7 (65). – С. 53-59.

4. Халимов Г.З. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов / Г.З. Халимов, А.В. Северинов // Системы управления и связь. – Х.: ХВУ, 1996. – С. 116-119.

5. 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.

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

7. Rao T.R.N. Private-key algebraic-coded cryptosystem. Advances in Cryptology. / T.R.N. Rao, K.H. Nam // CRYPTO 86, New York. – NY: Springer. – P. 35-48.

8. Стасев Ю.В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю.В. Стасев, А.А. Кузнецов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – К: НАНУ. – 2005. – №3. – С. 47-57.

9. Кузнецов А.А. Каскадные кодовые схемы защиты информации / А.А. Кузнецов, В.И. Грабчак, С.П. Евсеев // Системи обробки інформації. – Х.: ХУ ПС, 2005. – Вип. 9 (49). – С. 206-211.

10. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования / А.А. Кузнецов // Всеукр. меж вед. науч.-техн. сб. – Х.: ХТУРЭ, 2003. – Вып.134. – С. 218-222.

11. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов / А.А. Кузнецов // Электронное моделирование: Международный научно-теоретический журнал. – К: НАНУ, РАН, 2004. – №2. – С. 27-38.

12. Blake Ian. Algebraic – Geometry Codes / Ian Blake, Chris Heegard, Tom Hoholdt, Victor K. W. Wei // IEEE Trans. Info. Theory. – October 1998. – Vol. IT-44. – P. 2596-2618.

13. 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.

14. 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. – Х.: ХУ ПС, 2007. – Вип. 8 (66). – С. 134-139.

15. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.

16. Науменко М.І. Теоретичні основи та методи побудови алгебраїчних блокових кодів: монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов. – Х.: ХУ ПС, 2005. – 267 с.

Надійшла до редколегії 25.04.2011

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. Кожедуба, Харків.

СХЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ МАК-ЭЛЛИСА ИЗ АЛГЕБРОГЕОМЕТРИЧЕСКИМИ КОДАМИ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ

В.И. Грабчак, И.В. Пасько

В статье исследуются вопросы построения кодовых схем защиты информации доказательной устойчивости Мак-Эллиса с использованием алгеброгеометрических кодов на пространственных кривых, которые задаются в проективной пространстве P^3 совместимыми решениями совокупности двух однородных уравнений от четырех переменных, применение которых позволит интегрировано обеспечить достоверность и конфиденциальность информации в телекоммуникационных системах. Приведен пример их практической реализации.

Ключевые слова: *кодовые схемы защиты информации, схема Мак-Эллиса, алгеброгеометрические коды на пространственных кривых.*

PATTERNS OF INFORMATION MAK-ELLIS OF ALGEBRAIC CODES ON SPACE CURVES

V.I. Grabchak, I.V. Pasko

This article investigates the issues of building code information protection schemes evidence of stability Mack Ellis with Algebraic Codes on space curves, which are defined in the projective space P^3 compatible solutions together two homogeneous equations in four variables, the use of which will integrate to ensure authenticity and confidentiality of information in telecommunication systems. An example of their practical implementation.

Keywords*: coding scheme information protection scheme Mack Ellis, Algebraic Codes for space curves.*