ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ СИСТЕМ ОЗБРОЄННЯ

УДК 621.391

Ю.В. Стасєв, О.О. Кузнецов, В.І. Грабчак, С.П. Євсєєв

КАСКАДНІ СХЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА АЛГЕБРОГЕОМЕТРИЧНИХ КОДАХ

Розглядаються каскадні кодові конструкції й секретні системи, побудовані шляхом маскування кодів зовнішнього ступеня узагальненого каскадного коду. Досліджуються кодові схеми захисту інформації на алгеброгеометричних кодах.

Постановка проблеми та аналіз літератури

Ефективним механізмом забезпечення вірогідності й інформаційної скритності передачі даних в АСУВ є кодові схеми захисту інформації [1, 2]. Це секретні системи, побудова яких ґрунтується на маскуванні алгебраїчних блокових кодів зі швидкими алгоритмами декодування під випадковий код і зведенні задачі зламування секретної системи до теоретико-складнісної задачі декодування випадкового коду [3].

Перспективним напрямком у розвитку алгебраїчної теорії кодування є розробка лінійних блокових кодів за алгебраїчними кривими (алгеброгеометричних кодів). У [4, 5] показано, що теорія їх побудови узагальнює більшість відомих алгебраїчних кодів, таких, наприклад, як великий клас циклічних кодів, у тому числі кодів Боуза-Чоудхурі-Хоквінгема, кодів Ріда-Соломона та їх узагальнень, альтернантних кодів, у тому числі кодів Гоппи, Срівестави та ін. У [6] показано, що використання алгеброгеометричних кодів для передачі даних по дискретних каналах зв'язку дозволяє одержати істотний енергетичний виграш від кодування. У [1] запропоновані кодові схеми захисту інформації, побудовані на алгеброгеометричних кодах. Основним недоліком таких конструкцій є висока порівняно з блочно-симетричними шифрами складність формування і декодування кодограм. Перспективним напрямком є дослідження каскадних кодових конструкцій і побудованих на їх основі секретних систем [2].

Таким чином, розробка каскадних кодових схем захисту інформації з алгеброгеометричними кодами є актуальною.

Мета статті – розгляд каскадних кодових конструкції й секретних систем, побудованих шляхом маскування кодів зовнішнього ступеня узагальненого каскадного коду; дослідження кодових схем захисту інформації на алгеброгеометричних кодах.

Основний матеріал

Лінійні коди на алгебраїчних кривих. Алгеброгеометричні коди як лінійні системи на алгебраїчних кривих уперше були запропоновані В.Д. Гоппою [7]. Коди, побудовані за кривими з великою кількістю точок порівняно з родом, лежать вище межі Варшамова-Гілберта [8]. Наведемо з невеликими змінами загальну схему побудови алгеброгеометричних кодів.

Нехай $X(GF(q))$ – множина точок кривої X над скінченним полем $GF(q)$, $N = |X(GF(q))|$ – їх кількість. Кількість N точок кривої X над $GF(q)$ обмежена зверху виразом Хассе-Вейля [7, 8]

$$N \le 2g\sqrt{q} + q + 1,$$

де $g = g(X)$ – рід кривої.

Нехай C – клас дивізорів на X ступеня α. Тоді C задає відображення $\varphi : X \to P^m$, набір генераторних функцій $y_i = \varphi(x_i)$ задає алгеброгеометричний код довжиною $n \le N$.

Кодові характеристики (n, k, d) пов'язані співвідношенням [7, 8]

$$k + d \ge n - g + 1.$$

Якщо $2g - 2 < \alpha \le n$, код пов'язаний характеристиками

$$(n,\ \alpha - g + 1,\ d),\quad d \ge n - \alpha.$$

Дуальний до нього код також є алгеброгеометричними характеристиками

$$(n, n - \alpha + g - 1, d_\perp),\ d_\perp \ge \alpha - 2g + 2.$$

Розглянемо варіант побудови алгеброгеометричного коду, заданого через породжувальну матрицю. Скористаємося таким визначенням [9].

Алгеброгеометричний код над $GF(q)$ побудований через відображення кривої X вигляду $\varphi: EC \to P_{k-1}$. Це лінійний код довжиною $n \le N$, кодові слова $C(c_0, c_1, \ldots, c_{n-1})$ якого задаються рівністю

$$\sum_{j=0}^{k-1} I_j F_j(P_i) = c_i, \qquad (1)$$

де $P_i(X_i, Y_i, Z_i)$ – проективні точки кривої X, тобто (X_i, Y_i, Z_i) – розв′язання однорідного алгебраїчного рівняння, що задають криву X, $i = \overline{1,n}$;

$F_j(P_i)$ – значення генераторних функцій у точках кривої.

Це визначення рівносильне матричному представленню алгеброгеометричного коду:

$$\mathbf{G}\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}),$$

де **G** – породжувальна матриця розмірності k×n, $k = \alpha - g + 1$, $\alpha = \deg X \cdot \deg F$.

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

Кодове слово, у цьому випадку, може бути сформоване за правилом (1) або в матричній формі як добуток інформаційного вектора-рядка на породжувальну матрицю

$$\left\| \mathbf{c}_j \right\|_n = \mathbf{G} \left\| I_i \right\|_k^T = \left\| F_i(P_j) \right\|_{n,k} \left\| I_i \right\|_k^T.$$

Розглянутий алгоритм побудови алгеброгеометричних кодів може бути ефективно використаний при формуванні кодограм у каскадних кодових схемах захисту інформації.

Каскадні кодові схеми захисту інформації. Для побудови каскадної кодової схеми зафіксуємо узагальнений каскадний код порядку m. За визначенням [10] алгебраїчно заданий узагальнений каскадний код порядку m однозначно визначається n_2 квадратними двійковими матрицями $\mathbf{H}_0^j$, $j = \overline{1,n_2}$ порядку n_1 (задаючих (n_1, k_i, d_{1i}) коди першого ступеня) і $m+1$ груповими над $GF(2^{a_i})$, $i = \overline{1,m+1}$ кодами другого ступеня з параметрами (n_2, b_i, d_{2i}). Величини $a_i > 0$ і $b_i \geq 0$, що визначають внутрішню структуру узагальненого каскадного (n,k,d) коду, вибираються довільно, при цьому (n,k,d) параметри задовольняють такі співвідношення:

$$n = n_1 n_2; \quad k = \sum_{i=1}^{m+1} a_i b_i;$$

$$d \geq \begin{cases} \min\left\{ d_{1i} d_{2i} : i = \overline{1,m} \right\} & \text{при } b_{m+1} = 0; \\ \min\left\{ d_{2m+1}, d_{1i} d_{2i} : i = \overline{1,m} \right\} & \text{при } b_{m+1} \neq 0 \end{cases}$$

і виконується рівняння

$$\sum_{i=1}^{m+1} a_i = n_1. \qquad (4)$$

Формально, каскадна кодова схема за узагальненим каскадним (n, k, d) кодом порядку m складається із сукупності таких множин [2]:

множина відкритих текстів

$$M = \{M_1, M_2, ..., M_{q^k}\};$$

де кожне M_i являє собою інформаційний блок вигляду

$$\begin{aligned} M_i = \{&(I_{1,1}, I_{1,2}, ..., I_{1,a_1}), (I_{2,1}, I_{2,2}, ..., I_{2,a_1}), ..., \\ &(I_{b_1,1}, I_{b_1,2}, ..., I_{b_1,a_1}), \\ &(I_{1,1}, I_{1,2}, ..., I_{1,a_2}), (I_{2,1}, I_{2,2}, ..., I_{2,a_2}), ..., \\ &(I_{b_2,1}, I_{b_2,2}, ..., I_{b_2,a_2}), ..., \\ &(I_{1,1}, I_{1,2}, ..., I_{1,a_{m+1}}), (I_{2,1}, I_{2,2}, ..., I_{2,a_{m+1}}), ..., \\ &(I_{b_{m+1},1}, I_{b_{m+1},2}, ..., I_{b_{m+1},a_{m+1}})\}; \end{aligned}$$

множина криптограм

$$E = \{E_1, E_2, ..., E_{q^k}\},$$

де кожне E_i являє собою кодове слово вигляду

$$E_i = C_i + e_i,$$

тобто суму кодового слова узагальненого каскадного коду з випадковим вектором помилки e_i, причому

$$\begin{aligned} C_i = \{&(C_{1,1}, C_{1,2}, ..., C_{1,a_1}), (C_{2,1}, C_{2,2}, ..., C_{2,a_1}), ..., \\ &(C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_1}), \\ &(C_{1,1}, C_{1,2}, ..., C_{1,a_2}), (C_{2,1}, C_{2,2}, ..., C_{2,a_2}), ..., \\ &(C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_2}), ..., \\ &(C_{1,1}, C_{1,2}, ..., C_{1,a_{m+1}}), (C_{2,1}, C_{2,2}, ..., C_{2,a_{m+1}}), ..., \\ &(C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_{m+1}})\} \end{aligned}$$

або

$$\begin{aligned} C_i = \{&(\gamma_{1,1}, \gamma_{1,2}, ..., \gamma_{1,n_2}), (\gamma_{2,1}, \gamma_{2,2}, ..., \gamma_{2,n_2}), ..., \\ &(\gamma_{m+1,1}, \gamma_{m+1,2}, ..., \gamma_{m+1,n_2})\}, \end{aligned}$$

де $\gamma_{i,j} = (C_{j,1}, C_{j,2}, ..., C_{j,a_i})$ – двійковий вектор довжини a_i.

Таким чином, кодограмою є вектор

$$\begin{aligned} E_i = \{&(\gamma^*_{1,1}, \gamma^*_{1,2}, ..., \gamma^*_{1,n_2}), \\ &(\gamma^*_{2,1}, \gamma^*_{2,2}, ..., \gamma^*_{2,n_2}), ..., \\ &(\gamma^*_{m+1,1}, \gamma^*_{m+1,2}, ..., \gamma^*_{m+1,n_2})\}, \end{aligned}$$

де $\gamma^*_{ij} = \gamma_{ij} + e_{ij}$;

$$\sum_{i=1}^{m+1} a_i = n_1;$$

e_{ij} – елементи випадкового вектора помилок довжини a_i (сеансовий ключ), що задовольняє системі обмежень

$$w(e_{i,1}, e_{i,2}, ..., e_{i,n_2}) \le t_{2i} = (d_{2i} - 1)/2;$$

множина прямих відображень

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_s\},$$

де $\varphi_i: M \to E$, $i = 1, 2, \ldots, s$;

множина зворотних відображень

$$\varphi_{-1} = \{\varphi_{1-1}, \varphi_{2-1}, \ldots, \varphi_{s-1}\},$$

де $\varphi_{i-1}: E \to M$, $i = 1, 2, \ldots, s$;

множина ключів, параметризуючих прямі відображення

$$K = \{K_1, K_2, ..., K_s\}, \text{ тобто } \varphi_i : M \xrightarrow{K_i} E,$$

де $K_i = \{\mathbf{G}_X^1, \mathbf{G}_X^2, ..., \mathbf{G}_X^{m+1}\}$ – множина генераторних матриць, що задають m + 1 замаскованих кодів зовнішнього ступеня;

множина ключів, параметризуючих обернені відображення

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\}, \text{ тобто } \varphi_i^{-1} : E \xrightarrow{K_i^*} M,$$

де

$$K_i^* = \{\{\mathbf{X}^1, \mathbf{P}^1, \mathbf{D}^1\}, \{\mathbf{X}^2, \mathbf{P}^2, \mathbf{D}^2\}, ..., \{\mathbf{X}^{m+1}, \mathbf{P}^{m+1}, \mathbf{D}^{m+1}\}\}$$

– множина матриць, що маскують m + 1 кодів зовнішнього ступеня.

Співвідношення параметрів каскадної кодової схеми встановлює така теорема [11].

Теорема 1. Нехай задана каскадна теоретико-кодова схема за узагальненим каскадним кодом порядку m шляхом маскування всіх його кодів другого ступеню. Тоді об′єм ключа (у бітах) прямого відображення задається виразом

$$l_K = n_2 \sum_{j=1}^{m+1} b_j a_j, \qquad (5)$$

об′єм ключа (у бітах) оберненого відображення задається формулою

$$l_{K^*} = {n_2}^2 \sum_{i=1}^{m+1} {b_i}^2 a_j, \qquad (6)$$

довжина інформаційного блоку даних і довжина кодограми (у бітах) задаються відповідно виразами

$$l_M = \sum_{j=1}^{m+1} b_j a_j, \qquad (7)$$

$$l_E = n_1 n_2, \qquad (8)$$

а відносна швидкість передачі даних – формулою

$$R = \frac{1}{n_1 n_2} \sum_{j=1}^{m+1} b_j a_j. \qquad (9)$$

Теорема 1 установлює важливий взаємозв'язок між параметрами узагальненого каскадного коду й основними показниками каскадної теоретико-кодової схеми. Вирази (5) – (9) розкривають аналітичну залежність між кодовими характеристиками кодів зовнішнього ступеня узагальненого каскадного коду і характеристиками побудованої на їх основі криптосистеми.

Каскадні кодові схеми з алгеброгеометричними кодами. Проведемо дослідження каскадних кодових схем захисту інформації з алгеброгеометричними кодами на зовнішньому ступені узагальненого каскадного коду. Тоді у введеному вище формальному визначенні каскадних кодових схем як ключі, параметризуючі прямі відображення

$$K = \{K_1, K_2, ..., K_s\}, \text{ тобто } \varphi_i : M \xrightarrow{K_i} E,$$

будуть виступати множини генераторних матриць $K_i = \{\mathbf{G}_X^1, \mathbf{G}_X^2, ..., \mathbf{G}_X^{m+1}\}$, що задають m + 1 замаскованих алгеброгеметричних кодів, а як пряме і обернене відображення – процедури кодування та декодування узагальненого каскадного коду з замаскованими алгеброгеометричними кодами на зовнішньому ступені.

Позначимо символом g_j рід кривої, за якою будується алгеброгеметричний (n_2, b_j, d_{2j}) код зовнішнього ступеня узагальненого каскадного коду над $GF(2^{a_j})$, $j = \overline{1, m+1}$. Тоді параметри відповідної каскадної кодової схеми захисту інформації визначаються такою теоремою.

Теорема 2. Нехай задана каскадна кодова схема за узагальненим каскадним кодом порядку m шляхом маскування m + 1 алгеброгеометричних (n_2, b_j, d_{2j}) кодів зовнішнього ступеня над $GF(2^{a_j})$, $j = \overline{1, m+1}$. Тоді параметри секретної системи задаються виразами

$$l_K = (\alpha + 1)\, n_2 n_1 - n_2 \sum_{j=1}^{m+1} g_j a_j; \qquad (10)$$

$$l_{K^*} = (\alpha^2 + 1)\, {n_2}^2 n_1 - {n_2}^2 2\alpha \sum_{j=1}^{m+1} g_j a_j; \qquad (11)$$

$$l_M = (\alpha + 1) n_1 - \sum_{j=1}^{m+1} g_j a_j; \qquad (12)$$

$$l_E = n_1 n_2; \qquad (13)$$

$$R = \frac{(\alpha + 1)}{n_2} - \frac{1}{n_1 n_2} \sum_{j=1}^{m+1} g_j a_j. \qquad (14)$$

Доведення. Скористаємося результатами теореми 1, яка встановлює параметри для каскадної кодової схеми захисту інформації з замаскованими кодами зовнішнього каскаду. Підставимо параметри алгебро-геометричного коду, побудованого через породжувальну матрицю у співвідношення (5) – (9). Одержимо

$$l_K = n_2 \sum_{j=1}^{m+1}(\alpha - g_j + 1)a_j =$$

$$= n_2(\alpha+1)\sum_{j=1}^{m+1} a_j - n_2 \sum_{j=1}^{m+1} g_j a_j;$$

$$l_{K^*} = n_2^2 \sum_{j=1}^{m+1} (\alpha - g_j + 1)^2 a_j =$$

$$= n_2^2 \sum_{j=1}^{m+1} (\alpha^2 - 2\alpha g_j + 1)\, a_j =$$

$$= n_2^2 \sum_{j=1}^{m+1} (\alpha^2 + 1)\, a_j - n_2^2 \sum_{j=1}^{m+1} 2\alpha g_j a_j =$$

$$= n_2^2(\alpha^2+1)\sum_{j=1}^{m+1} a_j - n_2^2 2\alpha \sum_{j=1}^{m+1} g_j a_j;$$

$$l_M = \sum_{j=1}^{m+1}(\alpha - g_j + 1)\, a_j = (\alpha+1)\sum_{j=1}^{m+1} a_j - \sum_{j=1}^{m+1} g_j a_j\ ;$$

$$R = \frac{1}{n_1 n_2}\sum_{j=1}^{m+1}(\alpha - g_j + 1)a_j =$$

$$= \frac{(\alpha+1)}{n_1 n_2}\sum_{j=1}^{m+1} a_j - \frac{1}{n_1 n_2}\sum_{j=1}^{m+1} g_j a_j.$$

Скористаємося властивістю (1) з визначення узагальненого каскадного коду. Після підстановки одержимо вирази (10) – (14), що і завершує доведення.

Проведемо порівняльні дослідження варіантів маскування і необхідних обсягів ключових даних у каскадних кодових схемах захисту інформації з алгебро-геометричними кодами на зовнішньому ступені узагальненого каскадного коду. Для спрощення обчислень припустимо, що використовується основний варіант побудови і для всіх b_i та a_i виконуються рівності

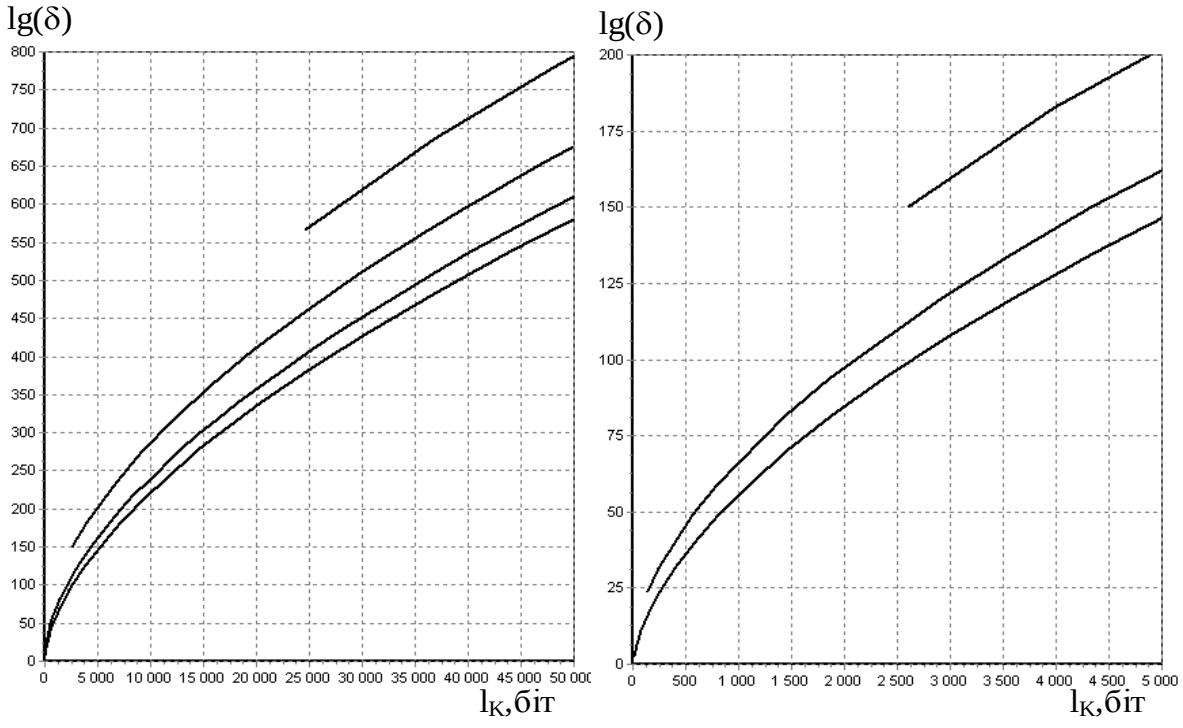
$$b_i = \frac{n_2}{2},\ a_i = \frac{n_1}{m+1},\ g_i = g,\ i = 1, \ldots, m+1...$$

Тоді

$$d_{2i} = n_2 - b_i - g_i + 1 = \frac{n_2}{2} - g_i + 1,\ \alpha = \frac{n_2}{2} + g_i - 1,$$

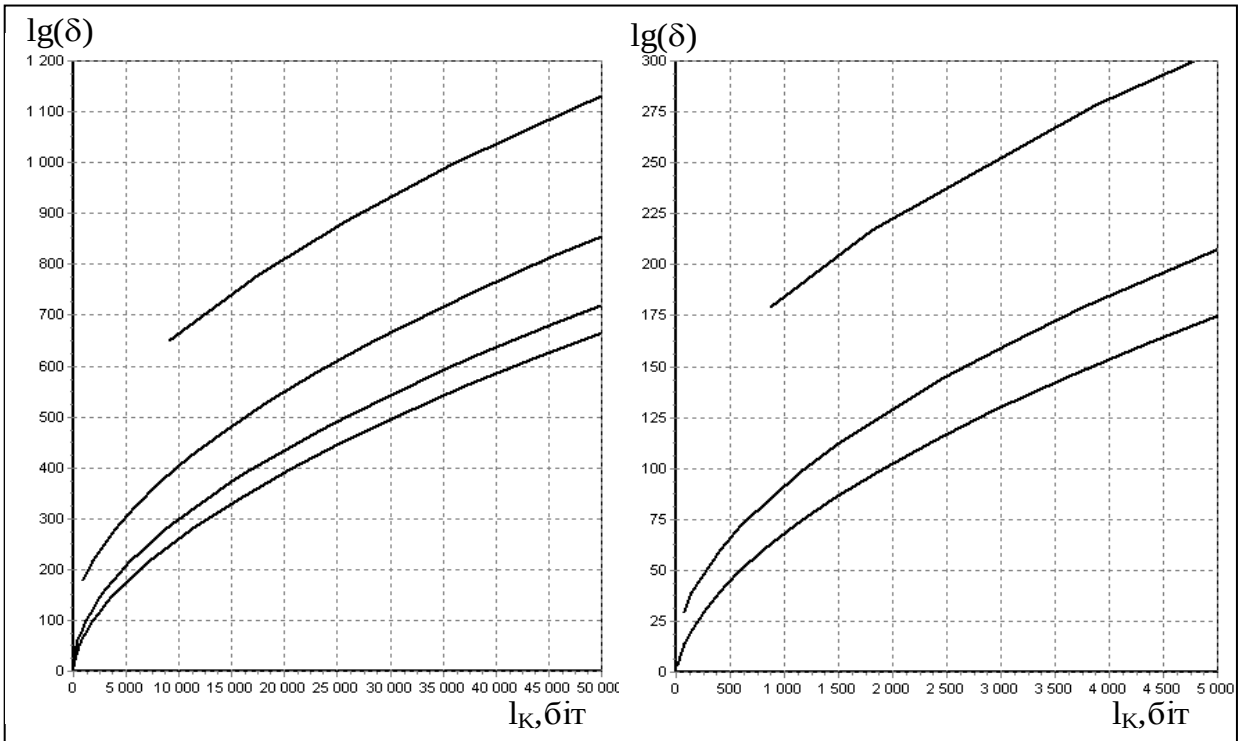
а вираз (10) запишеться у вигляді

$$l_K = \frac{(n_2)^2 n_1}{2} + g_i n_2 n_1 + n_2 n_1 - n_2 \sum_{j=1}^{m+1} g_j a_j =$$



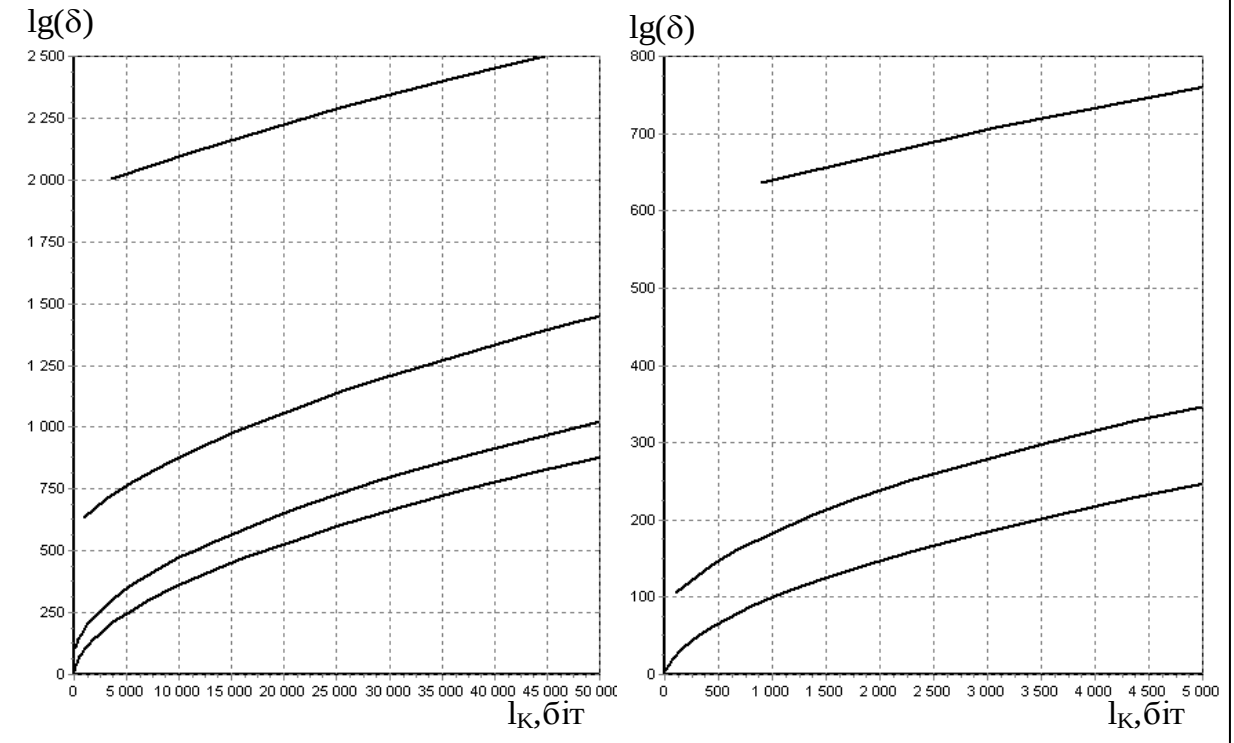
а б

Рис. 1. Верхня межа кількості переборів
при оптимальному статистичному опробовуванні супротивником при m = 3



а б

Рис. 2. Верхня межа кількості переборів
при оптимальному статистичному опробовуванні супротивником при m = 5



а б

Рис. 3. Верхня межа кількості переборів
при оптимальному статистичному опробовуванні супротивником при m = 10

$$= \frac{(n_2)^2 n_1}{2} + g n_2 n_1 + n_2 n_1 - n_2 (m+1)\, g n_1 =$$

$$= \frac{(n_2)^2 n_1}{2} + (1 - mg)\, n_2 n_1.$$

На рис. 1 – 3 наведені результати дослідження верхньої межі кількості переборів для оптимального статистичного опробовування супротивником для зламування каскадних кодових схем захисту інформації з замаскованими алгеброгеометричними кодами залежно від довжини ключа. Наведені залежності відповідають такому: 1 – застосування алгеброгеометричних кодів за кривими з $g = 0$ у P^2 (коди Ріда-Соломона та їх узагальнення); 2 – застосування алгеброгеометричних кодів за кривими з $g = 1$ у P^2 (коди за еліптичними кривими); 3 – застосування алгеброгеометричних кодів за кривими з $g = 3$ у P^2; 4 – застосування алгеброгеометричних кодів за кривими з $g = 6$ у P^2.

Розглянуті залежності для випадку $n_1 = n_2$ відповідають довжині ключів $l_K = 0...50000$ біт (а) та у великому масштабі для $l_K = 0...5000$ (б). Залежності наведені тільки для тих значень, при яких існують коди, відсутність лінії відповідає неможливості побудувати код з такими параметрами.

Аналіз наведених залежностей показує, що застосування алгеброгеометричних кодів на зовнішньому ступені узагальненого каскадного коду дозволяє побудувати потенційно стійку каскадну кодову схему захисту інформації з високими конструктивними показниками. Виграш зростає при переході до кривих з великою кількістю точок стосовно до роду кривої. Однак застосування таких кривих пов′язано зі збільшенням необхідного обсягу ключових даних. Виграш також зростає при переході до узагальнених каскадних кодів високого порядку, що узгоджується зі зробленими раніше висновками.

Висновки

Проведені дослідження показали, що перспективним напрямком у розвитку теорії секретних систем є каскадні кодові схеми захисту інформації. Розроблено каскадні кодові схеми захисту інформації з замаскованими алгеброгеометричними кодами на зовнішньому ступені узагальненого каскадного коду. Показано, що їх використання дозволяє побудувати потенційно стійку каскадну кодову схему захисту інформації з високими конструктивними показниками. Сформульована і доведена теорема, яка встановлює аналітичну залежність між параметрами алгеброгеометричних кодів на зовнішньому ступені узагальненого каскадного коду і параметрами побудованої на їх основі секретної системи. Встановлено, що найбільшу ефективність за критерієм максимуму кількості переборів оптимального статистичного опробовування супротивником дає застосування алгеброгеометричних кодів, побудованих за кривою з великою кількістю точок. Виграш зростає при переході до узагальнених каскадних кодів високого порядку.

Перспективним напрямком подальших досліджень є розробка практичних алгоритмів формування і декодування кодограм у каскадних кодових схемах захисту інформації, вироблення практичних рекомендацій з використання розроблених конструкцій для забезпечення вірогідності й інформаційної скритності передачі даних в АСУВ.

СПИСОК ЛІТЕРАТУРИ

1. Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ: Междунар. науч.-теорет. журнал. –2005. – № 3. – С. 47 – 57.

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

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

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

5. Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Алгеброгеометричне узагальнення лінійних блокових кодів // Системи озброєння і військова техніка: Наук. журнал. – 2005. – № 2(2). – С. 15 – 31.

6. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов // Электронное моделирование: Междунар. науч.-теорет. журнал. – 2004. – № 2. – С. 27 – 38.

7. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 – 1290.

8. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы математики. – М.: ВИНИТИ, 1984. – Т. 25. – С. 209 – 257.

9. Кузнецов А.А., Северинов А.В., Лысенко В.Н., Науменко И.В. Алгоритм помехоустойчивого кодирования с использованием кодов по кривым Эрмита // Системи обробки інформації: Зб. наук. пр. – Х.: ХВУ, 2003. – № 6(28). – С. 181 – 186.

10. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды (Алгебраическая теория и сложность реализации). – М.: Связь, 1976. – 240 с.

11. Стасев Ю.В., Кузнецов А.А., Грабчак В.І., Ковтун В.Ю. Разработка теоретико-кодовых схем на обобщенных каскадных кодах // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС, 2006. – Вип. 2 (8). – С. 79 – 81.

Надійшла 30.01.2006

Рецензент: д-р фіз.-мат. наук професор С.В. Смєляков, Харківський університет Повітряних Сил ім. Івана Кожедуба.