УДК 681.3.06

д.т.н., проф. Дудикевич В.Б. (НУ «ЛП», Львів),
д.т.н., проф. Кузнєцов О.О. (СНС Харківського УПС),
Томашевський Б.П. (НЦ СВ Академії СВ)

КРИПТО-КОДОВИЙ ЗАХИСТ ІНФОРМАЦІЇ З НЕДВІЙКОВИМ РІВНОВАГОВИМ КОДУВАННЯМ

1. Постановка проблеми в загальному вигляді і аналіз літератури

Проведені дослідження показали, що перспективним напрямом в розвитку методів і механізмів захисту інформації є інтегровані крипто-кодові засоби захисту інформації [1-6]. Їх побудова заснована на комплексному використанні методів завадостійкого кодування в режимі маскування від порушника швидкого правила декодування і укриття, таким чином, від не уповноваженого користувача повідомлень змістовного характеру які передаються. Найбільшу ефективність захисту даних які передаються в комп'ютерних системах і мережах забезпечують несиметричні крипто-кодові засоби захисту інформації, побудовані на недвійкових завадостійких кодах і допускають функціонування в режимі виявлення помилок і автоматичного перезапиту даних які передаються [5, 6].

В даній статті розглядається формальний математичний опис крипто-кодових засобів захисту інформації, досліджується процес крипто-кодового перетворення інформації і передачі даних в режимі виявлення помилок і автоматичного перезапиту. Вводиться формальне математичне визначення крипто-кодових засобів захисту інформації з використанням недвійкових рівновагових кодів, розробляються схеми перетворення інформації запропонованими засобами захисту. Запропоновані механізми крипто-кодового захисту інформації дозволяють реалізувати обмін конфіденційними повідомленнями з використанням відкритих ключових даних і інтегровано забезпечити потрібні показники безпеки і достовірності передачі даних.

2. Математична модель крипто-кодових засобів захисту інформації в режимі виявлення помилок і автоматичного перезапиту. Розглянемо процес забезпечення безпеки і достовірності передачі даних з використанням крипто-кодових засобів захисту інформації в режимі виявлення помилок які виникли, і автоматичного перезапиту, дослідимо особливості використання математичного апарату завадостійкого кодування для інтегрованого рішення задач підвищення безпеки і достовірності передачі даних в комп'ютерних системах і мережах.

Математична модель несиметричної крипто-кодової системи захисту інформації задається сукупністю наступних елементів [4, 5]:

- множина відкритих текстів

$$M = \{M_1, M_2, ..., M_m\}, \text{ де } M_i = e = \{e_0, e_1, ..., e_{n-1}\}, \ \forall e_j \in GF(q); \qquad (1)$$

- множина закритих текстів

$$E = \{E_1, E_2, ..., E_m\}, \text{ де } E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}}), \ \forall S_{X_j} \in GF(q); \qquad (2)$$

- множина прямих відображень

$$\varphi = \{\varphi_1, \varphi_2, ..., \varphi_s\}, \text{ де } \varphi_i : M \to E, \ i = 1,2,...,s; \qquad (3)$$

- множина зворотних відображень

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\}, \text{ де } \varphi_i^{-1} : E \to M, \ i = 1,2,...,s; \qquad (4)$$

- множина ключів, які параметризують прямі відображення

$$K = \{K_1, K_2, ..., K_s\} = \{H_X^1, H_X^2, ..., H_X^s\}; \qquad (5)$$

де H_X^i - перевірочна $n\times(n-k)$ матриця замаскованого під випадковий код алгебраїчного блокового (n,k,d) коду з елементами з $GF(q)$, тобто

$$\varphi_i : M \xrightarrow{K_i} E ; i = 1,2,...,s ;$$

– множина ключів, які параметризують зворотні відображення

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\}, \quad (6)$$

$$\{X,P,D\}_i = \{X^i, P^i, D^i\},$$

де X^i - маскуюча не вироджена випадково сформована джерелом ключів $(n-k)\times(n-k)$ матриця з елементами з $GF(q)$; P^i - перестановочна випадково сформована джерелом ключів $n\times n$ матриця з елементами з $GF(q)$; D^i - діагональна сформована джерелом ключів $n\times n$ матриця з елементами з $GF(q)$, тобто

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} M , i = 1,2,...,s ,$$

причому складність виконання зворотного відображення φ_i^{-1} без знання ключа $K_i^* \in K^*$ зв'язана з рішенням теоретико-складного завдання декодування випадкового коду (коду загального положення) [3].

Таким чином, аналітичні вирази (1) – (6) формалізовано описують основні структурні елементи і функціональні залежності між основними компонентами секретної системи. Алгебраїчний блоковий (n,k,d) код *C* з швидким алгоритмом декодування маскується під випадковий *(n, k, d)* код *C** безпосередньо перемноженням перевірочної матриці H коду *C* на матриці маскування які зберігаються в таємниці X^u, P^u и D^u [3]:

$$H_X^u = X^u \cdot H \cdot P^u \cdot D^u , u \in \{1,2,...,s\}, \quad (7)$$

де H - перевірочна $n\times(n-k)$ матриця алгебраїчного блокового (n,k,d) коду з елементами із $GF(q)$.

Ключ H_X^u, $u \in \{1,2,...,s\}$ із (7) може бути відкритим, і система захисту інформації в цьому випадку може бути використана в режимі шифрування з відкритим ключем для систем передачі даних в режимі автоматичного перезапиту.

Формування закритого тексту $E_j \in E$ по введеному відкритому тексту $M_i \in M$ і заданому ключі H_X^u, $u \in \{1,2,...,s\}$ здійснюється шляхом формування синдромної (в термінах завадостійкого колування) послідовності S_{X_j}, яка відповідає рівноваговій послідовності $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$:

$$S_{X_j} = \varphi_u\left(M_i, H_X^u\right) = M_i \cdot \left(H_X^u\right)^T , \quad (8)$$

причому вага Хеммінга (число ненульових елементів) вектору M_i не перевищує виправлячу здатність алгебраїчного блокового (n,k,d) коду який використовується:

$$\forall i : 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor . \quad (9)$$

Потужність множин M і E визначається допустимим спектром ваги $w(M_i)$ в виразі (9), тобто в загальному випадку (для всіх допустимих значень $w(M_i)$) маємо:

$$m = \sum_{i=0}^{t} (q-1)^i \cdot C_n^i ,$$

де C_n^i - біноміальний коефіцієнт, $C_n^i = \dfrac{n!}{i! \cdot (n-1)!}$.

В роботах [3-5] показано, що найбільш доцільно величину $w(M_i)$ вибирати в відповідності з потрібним значенням безпеки передачі даних.

Тоді, для

$$w(M_i) = const = w(e)$$

маємо:

$$m = (q-1)^{w(e)} \cdot C_n^{w(e)},$$

а послідовності $M_i = \{e_0, e_1, ..., e_{n-1}\}$ з множини $M = \{M_1, M_2, ..., M_m\}$ формуються як результат деякого відображення ψ, реалізованого шляхом надмірного кодування недвійковими рівноваговими кодами без надмірних інформаційних послідовностей.

Закритий текст $E_j \in E$ однозначно відповідає вектору $M_i = \{e_0, e_1, ..., e_{n-1}\}$, що забезпечується однозначністю результату матричного множення (8).

На прийомній стороні уповноважений користувач, який знає правило маскування (набор матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) формує кодову послідовність $c^*_{X_i}$ як одне (любе) з можливих рішень рівняння

$$S_{X_i} = c^*_{X_i} \cdot H^T_{X_j},$$

тобто находить такий вектор $c^*_{X_i}$, який розкладається на суму

$$c^*_{X_i} = c_{X_i} + M_i,$$

де c_{X_i} - одне (любе) із можливих кодових слів замаскованого (n,k,d) коду з перевірочною матрицею $H^T_{X_j}$, тобто $c_{X_i} \cdot H^T_{X_j} = 0$.

Дальше, уповноважений користувач, використовуючи набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$ формує вектор

$$\bar{c}^* = c^*_X \cdot (D^u)^{-1} \cdot (P^u)^{-1},$$

тобто демаскує кодову послідовність $c^*_{X_i}$.

Після підстановки отримаємо рівність:

$$\begin{aligned} \bar{c}^* &= c^*_X \cdot (D^u)^{-1} \cdot (P^u)^{-1} = (c_{X_i} + M_i) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= c_{X_i} \cdot (D^u)^{-1} \cdot (P^u)^{-1} + M_i \cdot (D^u)^{-1} \cdot (P^u)^{-1}. \end{aligned} \qquad (10)$$

За визначенням вектор c_{X_i} є кодовим словом замаскованого (n,k,d) коду з перевірочною матрицею $H^T_{X_j}$, тобто виконується рівність:

$$c_{X_i} \cdot H^T_{X_j} = 0.$$

Відповідно, справедлива також рівність

$$c_{X_i} = I \cdot G^T_{X_j},$$

для деякого I і виродженої матриці $G^T_{X_j}$ замаскованого (n,k,d) коду, причому

$$G_{X_j} \cdot H^T_{X_j} = 0$$

Таким чином, перший доданок в виразі (10) задає демаскування кодове слово вихідного (n,k,d) коду з перевірочною матрицею

$$H^u = H_{X_j} \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = X^u \cdot H$$

і відповідною виродженою матрицею

$$G^u \cdot \left(H^u\right)^T = 0.$$

Варто відмітити, що матриці $H^u = X^u \cdot H$ і H задають один і той же початковий алгебраїчний блоковий (n,k,d) код лише з цією різницею, що для випадку з H^u інформаційна послідовність при кодуванні додатково множиться на не вироджену матрицю X^u (не виродженість забезпечує зворотність перетворень). Іншими словами уповноважений користувач, який сформував вектор $\bar{c}^*$ по виразу (10), має можливість примінити швидкий (поліноміальної складності) алгоритм завадостійкого декодування і сформувати таким чином вектор

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$$

і вектор

$$M^u_i = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

Для відновлення інформаційної рівновагової послідовності M_i достатньо знову помножити вектор M^u_i на матриці масскування D^u і P^u, але в іншому порядку:

$$M_i = M^u_i \cdot P^u \cdot D^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u = M_i.$$

Таким чином, матриця X^u при розшифруванні інформаційного повідомлення не використовується.

Порушник, не знаючи правил маскування, яке задається секретним ключем (набором матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$), для дешифрування повідомлення змушений використовувати складний алгоритм декодування випадкового коду (в загальному випадку алгоритм експоненціальної складності) [3-5].

Таким чином, процес формування криптограми в розглянутій крипто-кодовій системі захисту інформації виконується послідовно алгоритмами рівновагового кодування і кодування замаскованими алгебраїчними блоковими кодами. Підвищення безпеки передачі даних досягається за рахунок приховування в тайні від не уповноваженого користувача (противника) швидкого правила декодування алгебраїчних блокових кодів. Потрібна криптографічна стійкість забезпечується зведенням задачі встановлення інформаційних даних без знання секретного ключа до рішення теоретико-складної задачі декодування випадкового коду. В цей час, проведені дослідження розглянутої математичної моделі несиметричної крипто-кодової системи захисту інформації показали, що застосовані алгебраїчні блокові коди не використовуються для виявлення і/або виправлення помилок. Люба помилка яка виникла при передачі даних спотворить синдромну послідовність

$E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}})$, яка однозначно зв'язана з рівноваговим вектором $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$ і приховає його змістовний характер. Другими словами, помилки які появилися в результаті передачі даних приведуть до спотворення змістовного характеру повідомлень які передаються.

Проведений аналіз основних етапів формування криптограми яка розглядається в крипто-кодовій системі захисту інформації показав, що забезпечення потрібної достовірності передачі даних і ефективного контролю помилок (в режимі виявлення і автоматичного перезапиту) може бути покладено на контур рівновагового кодування. Для підвищення достовірності передачі даних рекомендується використовувати виявляючу здатність рівновагового коду яка застосовується для контролю помилок які виникли в результаті процесу передачі по каналам зв'язку.

Розглянемо варіант побудови крипто-кодової системи захисту інформації в режимі виявлення помилок і автоматичного перезапиту з рішенням задачі ефективного контролю помилок в асиметричних каналах передачі даних на рівні процедур рівновагового кодування, які застосовуються.

З точки зору наведених вище суджень і позначень *введемо формальне математичне визначення крипто-кодової системи захисту інформації в режимі виявлення помилок і автоматичного перезапиту* наступним чином:

– множина відкритих текстів

$$M = (M_1, M_2, ..., M_{q^m}),$$

де

$$M_i = (I_0, I_1, ..., I_{m-1}),\ \forall I_j \in GF(q),$$

причому кожному M_i можна однозначно зіставити вектор

$$\varepsilon_i = (e_0, e_1, ..., e_{n-1}),\ \forall e_j \in GF(q),\ w(\varepsilon_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor,$$

із множини $\Phi = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_{q^m})$, тобто виконується відображення

$$\psi : M \to \Phi,$$

так, що для $\forall i$ справедливо

$$\varepsilon_i = \psi(M_i),$$

де ψ задається процедурою недвійкового (по основі q) рівновагового кодування [7-9];

– множина криптограм

$$E = (E_1, E_2, ..., E_{q^m}),$$

де

$$E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}}),\ \forall S_{X_j} \in GF(q),$$

причому кожному E_i можна однозначно зіставити вектор ε_i;

– множина прямих відображень

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

де

$$\varphi_j: M \to E,\ j = 1, 2, ..., s,$$

причому для $\forall j$ справедливо

$$E_i = \varphi_j(m_i);$$

– множина зворотних відображень

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\},$$

де

$$\varphi_j^{-1}: E \to M, j = 1, 2, ..., s,$$

причому для $\forall j$ справедливо

$$m_i = \varphi_j^{-1}(E_i);$$

– множина ключів, які параметризують прямі відображення

$$K = \{K_1, K_2, ..., K_s\} = \{H_X^1, H_X^2, ..., H_X^s\},$$

тобто

$$\varphi_j : M \xrightarrow{\mathrm{K_j}} E,\ E_i = \varphi_j(m_i, K_j);$$

– множина ключів, які параметризують зворотні відображення

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\},$$

тобто

$$\varphi_j^{-1} : E \xrightarrow{\mathrm{K_j^*}} M,\ m_i = \varphi_j^{-1}(E_i, K_j^*).$$

Виконання зворотного відображення φ^{-1}, тобто обчислення

$$m_i = \varphi_j^{-1}(E_i)$$

без знання ключа

$$K_j^* \in K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\}$$

пов’язано з рішенням теоретико-складного завдання декодування випадкового коду (коду загального положення).

Множина *M,* Φ , і *E* рівнопотужні, тобто

$$|M| = |\Phi| = |E| = q^m,$$

причому q^m не перевищує потужності рівновагового коду, тобто повної множини послідовностей довжини *n* і ваги $w(\varepsilon_i)$:

$$q^m \le C_n^{w(\varepsilon_i)},$$

звідси отримаємо:

$$m \le log_q\left(C_n^{w(\varepsilon_i)}\right).$$

Початковими даними при описі розглянутої крипто-кодової системи захисту інформації являються:

- недвійковий рівноваговий код над *GF(q)*, тобто множина послідовностей довжини *n* і ваги $w(\varepsilon_i)$;

- недвійковий алгебраїчний блоковий *(n, k, d)* код *C* над *GF(q),* тобто множина кодових слів $C_i \in C$ таких, що виконується рівність $C_i H^T = 0$, де *H* – перевірочна матриця алгебраїчного блокового коду;

- маскуючі матричні відображення, задані множиною матриць $\{X,P,D\}_i$, де *X* – не вироджена $k \times k$ матриця над *GF(q), P* – перестановочна $n \times n$ матриця над *GF(q)* з одним ненульовим елементом в кожній строчці і в кожному стовпці матриці, *D* – діагональна $n \times n$ матриця над *GF(q)* з ненульовими елементами на головній діагоналі.

На рис. 1. схематично зображені основні етапи формування криптограми, з вказаними методами кодування які використовуються.

Рис. 1. Схема формування криптограми в крипто-кодовій системі захисту інформації в режимі виявлення помилок і автоматичного перезапиту

Аналіз наведеної схеми показує, що забезпечення безпеки передачі даних покладається на контур алгебраїчного кодування блоковими кодами (нижня частина рисунка). В той же час при формуванні криптограми використовуються методи рівновагового кодування, які вносять надмірність в рівновагові послідовності які формуються (верхня частина рисунка). Внесену надмірність пропонується використовувати для виявлення помилок і підвищення достовірності передачі даних в режимі автоматичного перезапиту.

Схема процесу зворотного крипто-кодового перетворення (на прийомній стороні) приведена на рис. 2. На прийомній стороні уповноважений користувач формує кодову послідовність, яка відповідає прийнятій з каналу зв'язку шифрограмі. Використовуючи секретні ключові дані, уповноважений користувач демаскує кодову послідовність і застосовує швидкий алгоритм декодування (поліноміальної складності). Використовуючи матриці маскування (секретний ключ) формує рівновагову послідовність $\varepsilon_i = (e_0, e_1, ..., e_{n-1})$ і методами рівновагового декодування формує інформаційне повідомлення $M_i = (I_0, I_1, ..., I_{m-1})$.

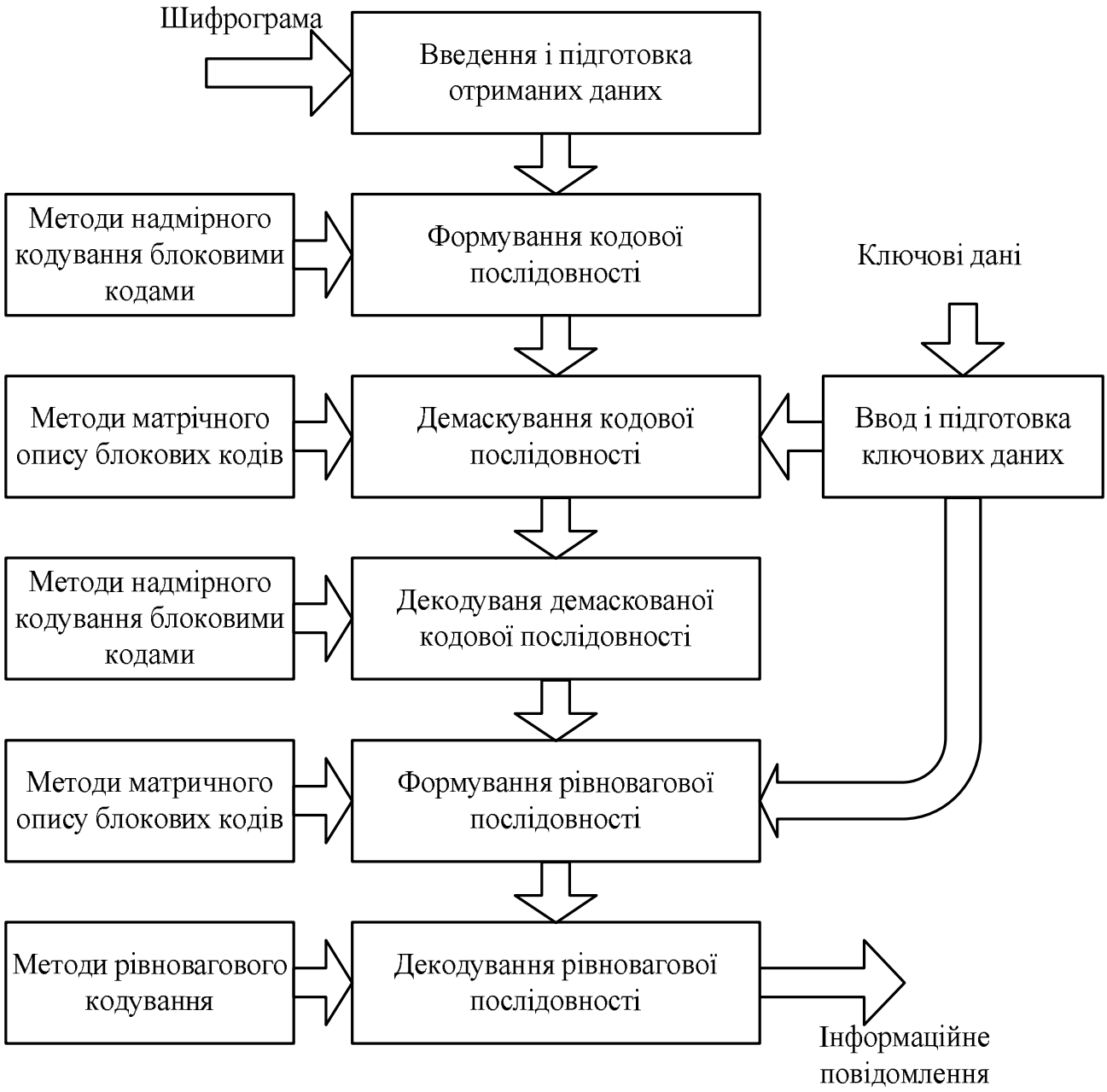

Рис. 2. Схема зворотного крипто-кодового перетворення
в режимі виявлення помилок і автоматичного перезапиту

Припустимо, що при передачі по каналу зв'язку криптограма яка передається спотворилась, тобто при впливі помилок в каналі передачі даних криптограма S_{X_i} яка передається на прийомній стороні прийнята з деякою помилкою $S_{X_i} + \delta$. Тоді уповноважений користувач на прийомній стороні, який знає правило маскування (набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) формує кодову послідовність $c^*_{X_i}$ як одне (будь-яке) з можливих рішень рівняння

$$S_{X_i} + \delta = c^*_{X_i} \cdot H^T_{X_j},$$

тобто находить такий вектор $c^*_{X_i} + \delta *$, який розкладається на суму

$$c^{*}_{X_i} + \delta^{*} = c_{X_i} + \varepsilon_i + \delta^{*},$$

де c_{X_i} - одне (будь-яке) з можливих кодових слів замаскованого (n,k,d) коду з перевірочною матрицею $H^T_{X_j}$, тобто. $c_{X_i} \cdot H^T_{X_j} = 0$, а δ^{*} - послідовність, відповідна помилці яка виникла в каналі зв'язку δ, тобто $\delta = \delta^{*} \cdot H^T_{X_j}$.

Уповноважений користувач, застосовує швидкий (поліноміальної складності) алгоритм завадостійкого декодування, формує суму рівновагового вектору $\varepsilon_i = (e_0, e_1, ..., e_{n-1})$ і вектору δ^{*}, тобто обчислює вектор $\varepsilon_i + \delta^{*}$. Очевидно, що при $\delta^{*} \neq 0$ застосування рівновагового декодера не дозволить відновити інформаційну послідовність $M_i = (I_0, I_1, ..., I_{m-1})$. Якщо ненульовий вектор δ^{*} змінить вагу послідовності, тобто, якщо $w(\varepsilon_i + \delta^{*}) \neq w(\varepsilon_i)$ декодер рівновагового коду видасть помилку декодування і запит на повторну передачу, тобто станеться виявлення помилки яка відбулася в каналі зв'язку і в режимі автоматичного перезапиту буде виконуватися повторна передача даної криптограми. Навпаки, при $w(\varepsilon_i + \delta^{*}) = w(\varepsilon_i)$ декодер рівновагового коду помилки яка виникла не виявить, його рішенням буде неправдиве інформаційне повідомлення.

Висновки

Таким чином, в результаті проведених досліджень отримано подальший розвиток математичного апарату крипто-кодового захисту інформації з використанням недвійкових рівновагових кодів і алгебраїчних блокових кодів в режимі виявлення помилок і автоматичного перезапиту. Запропоновано формальне математичне визначення крипто-кодової системи захисту інформації враховує особливості формування криптограм з використанням недвійкових рівновагових кодів і їх зворотного крипто-кодового перетворення на прийомній стороні для підвищення безпеки і достовірності передачі даних в режимі виявлення помилок і автоматичного перезапиту.

Перспективним напрямом подальших досліджень є оцінка ймовірностей подій $w(\varepsilon_i + \delta^{*}) = w(\varepsilon_i)$ і $w(\varepsilon_i + \delta^{*}) \neq w(\varepsilon_i)$, оцінка ефективності передачі даних з врахуванням досягнутих показників безпеки і достовірності передачі даних в комп'ютерних системах і мережах. Крім того, введене формальне математичне визначення несиметричної крипто-кодової системи захисту інформації на недвійкових рівновагових кодах і алгебраїчних блокових кодах в режимі автоматичного перезапиту дозволяє перейти до розробки алгоритмів формування і розшифрування криптограм, обґрунтуванню рекомендацій по їх програмно-апаратній реалізації

Список літератури

1. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

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

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

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

5. Кузнецов А.А. Несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал – Х.: ХАИ. – 2007.– №8(27) – С.130-144.

Досліджуються механізми комплексного забезпечення безпеки і достовірності передачі даних в комп'ютерних системах і мережах, засновані на інтеграції криптографічних засобів захисту інформації і канального (завадостійкого) кодування. Вводиться формальне математичне визначення крипто-кодових засобів захисту інформації з використанням недвійкових рівновагових кодів, розробляються схеми перетворення інформації запропонованими засобами захисту.

Ключові слова: криптографічні засобі, кодування, крипто-кодові засоби захисту.

Исследуются механизмы комплексного обеспечения безопасности и достоверности передачи данных в компьютерных системах и сетях, основанные на интеграции криптографических средств защиты информации и канального (помехоустойчивого) кодирования. Вводится формальное математическое определения крипто-кодовых средств защиты информации с использованием недвоичных равновесных кодов, разрабатываются схемы преобразования информации предложенными средствами защиты.

Ключевые слова: криптографические средства, кодирование, крипто-кодовые средства защиты.

The article explores the mechanisms of complex safeguarding of security and the trustworthiness of the datas' transmitting in the computer systems and resources that are based on the integration of cryptographic means of information protection and channel (antijamming) of encoding. The research defines mathematical definition of the cryptocoded means of information protection with non binary egnilibrium codes utihzation and also the schenes of the information transformation are worked out with the proposed means of protection.

Key words: cryptomaterial, coding, crypto-code security facilities.

Надійшла 24.12.2009

УДК 621.391:519.2

д.т.н., проф. Алексейчук А. Н., Шевцов А. С. (НТУУ «КПИ»)

ВЕРХНИЕ ОЦЕНКИ НЕСБАЛАНСИРОВАННОСТИ БИЛИНЕЙНЫХ АППРОКСИМАЦИЙ РАУНДОВЫХ ФУНКЦИЙ БЛОЧНЫХ ШИФРОВ ГОСТ 28147-89 И "КАЛИНА"

Введение

Одной из важнейших задач современного криптоанализа является разработка общих методов оценки и обоснования стойкости блочных шифров относительно статистических атак (разностых, линейных, билинейных и др. [1 – 6]). Как правило, решение этой задачи приводит к необходимости построения оценок параметров, вычисление точных значений которых практически не осуществимо.

Основным параметром, характеризующим обоснованную стойкость блочного шифра относительно линейного (билинейного) метода криптоанализа, является максимальное значение несбалансированности его линейных (билинейных) аппроксимаций [3, 4, 6]. При этом нахождение приемлемых (по точности и сложности вычислений) верхних оценок указанного параметра, как правило, представляет собой нетривиальную задачу, которая, за редким исключением [7], не поддается решению известными методами. В этой связи при исследовании стойкости блочных шифров относительно линейного (билинейного) метода криптоанализа обычно ограничиваются построением оценок вероятностей линейных характеристик (билинейных аппроксимаций раундовой функции) данного блочного шифра. Отметим, что последняя задача также является нетривиальной и, в ряде случаев, требует развития известных и применения новых математических методов [7 – 14].

В настоящей статье решается задача построения верхних оценок параметров, характризующих способность раундовых функций шифров ГОСТ 28147-89 (далее – ГОСТ) [15], и "Калина" [16] противостоять билинейному методу криптоанализа. (Напомним, что ГОСТ является действующим в настоящее время стандартом, а "Калина" – кандидатом на Национальный стандарт шифрования Украины). С использованием общих теорем, доказанных в [14], получены численные оценки несбалансированности ряда билинейных