УДК 681.3.06

Б.П. Томашевський

Академія сухопутних військ Збройних Сил України, Львів

КРИПТО-КОДОВІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА НЕДВІЙКОВИХ РІВНОВАГОВИХ КОДАХ

Розглядаються несиметричні криптосистеми на алгебраїчних блокових кодах (крипто-кодові засоби захисту інформації) для побудови комплексних механізмів забезпечення безпеки і достовірності передавання даних. Розглядається формальний математичний опис несиметричних кодових криптосистем, досліджується процес крипто-кодового перетворення інформації. На основі недвійкового рівновагового кодування запропонований метод формування сеансових ключових даних який реалізується з використанням розроблених процедур рівновагового недвійкового кодування і дозволяє, адаптивно змінюючи вагу послідовностей, інтегровано забезпечувати потрібні показники безпеки і достовірності передавання даних у крипто-кодових системах захисту інформації.

Ключові слова: *несиметричні криптосистеми, рівновагове недвійкове кодування.*

Постановка проблеми у загальному вигляді та аналіз літератури

Проведенні дослідження [1 – 5] показали, що найбільш перспективним напрямом розвитку комплексних механізмів забезпечення потрібної безпеки і достовірності передавання даних є крипто-кодові системи захисту інформації, які дозволяють інтегрувати методи криптографічного перетворення і канального (завадостійкого) кодування даних, які передаються. Найбільшу ефективність захисту даних, що передаються, забезпечують несиметричні крипто-кодові засоби захисту інформації, побудовані на недвійкових завадостійких кодах з швидкими алгоритмами декодування (поліноміальної складності) [4, 5].

В даній статті розроблено крипто-кодові системи захисту інформації з раніше запропонованими [6 – 8] недвійковими рівноваговими кодами. Пропоновані механізми крипто-кодового захисту інформації дозволяють реалізувати обмін конфіденціальними повідомленнями з використанням відкритих ключових даних і інтегровано забезпечать потрібні показники безпеки і достовірності передавання даних.

1. Математична модель крипто-кодового захисту інформації

Формальний математичний опис секретних систем вперше подано в роботі відомого американського вченого К.Шеннона, який ввів абстрактний опис і формалізував аналітичними виразами процес криптографічного захисту інформації [9]. В роботах [4,5], за аналогією з класичними роботами Шеннона, введено формальний математичний опис несиметричних криптосистем на алгебраїчних блокових кодах (крипто-кодових засобів захисту інформації).

Розглянемо математичні моделі крипто-кодових засобів захисту інформації в різних режимах функціонування, дослідимо шляхи підвищення безпеки і достовірності передавання даних у комп'ютерних системах і мережах.

У відповідності з формальним математичним визначенням секретної системи, введеним в роботі К. Шеннона, секретна система абстрактно задається сукупністю таких множин: множина відкритих текстів M = {M1, M2, …, Mm}; множина закритих текстів E = {E1, E2, …, Em}; множина прямих відображень φ = {φ1, φ2, …, φs}, параметризованих відповідними ключами: $\phi_i : M \xrightarrow{K_i} E$; множина зворотних відображень φ-1 = {φ1-1, φ2-1, …, φs-1}, параметризованих відповідними ключами: $\phi_i^{-1} : E \xrightarrow{K_i^*} M$; множина ключів прямих відображень {K1, K2, …, Ks}; множина ключів зворотних відображень K* = {K1*, K2*, …, Ks*}.

Математична модель несиметричної крипто-кодової системи захисту інформації з використанням алгебраїчних блокових кодів, заданих через вироджену матрицю, формально задається сукупністю таких елементів [4, 5]:

– множина відкритих текстів

$$M = \{M_1, M_2, ..., M_{q^k}\}, \quad (1)$$

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

– множина закритих текстів

$$E = \{E_1, E_2, ..., E_{q^k}\}, \quad (2)$$

де $E_i = (c^*_{X_0}, c^*_{X_1}, ..., c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

– множина прямих відображень

$$\phi = \{\phi_1, \phi_2, ..., \phi_s\}, \quad (3)$$

де $\phi_i : M \to E$, $i = 1, 2, ..., s$;

– множина зворотних відображень

$$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\},$$

де $\phi_i^{-1} : E \to M$, $i = 1, 2, ..., s$;

– множина ключів, параметризованих прямими відображеннями

$$K = \{K_1, K_2, ..., K_s\} = \{G_X^1, G_X^2, ..., G_X^s\}, \quad (5)$$

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

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

– множина ключів, параметризованих зворотними відображеннями

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

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

де X^i - маскуюча не вироджена випадково сформована джерелом ключів $k \times k$ 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), точніше:

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

причому складність виконання зворотного відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ узгоджена з вирішенням теоретико-складної задачі декодування випадкового коду [3 – 5].

В даній несиметричній крипто-кодовій системі алгебраїчний (n, k, d) код C зі швидким алгоритмом декодування маскується під випадковий (n, k, d) код C* за допомогою множення виродженої матриці G коду C на маскуючі матриці, що зберігаються в таємниці X^u, P^u D^u [3-5]:

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

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

Ключ G_X^u, $u \in \{1, 2, ..., s\}$ може бути відкритим і система захисту інформації в даному випадку може бути використана в режимі шифрування з відкритим ключем для систем передавання даних у режимі прямого виправлення помилок.

Формування закритого тексту $E_j \in E$ по введеному відкритому тексту $M_i \in M$ і заданому ключу G_X^u, $u \in \{1, 2, ..., s\}$ виконується шляхом формування кодового слова замаскованого коду з додаванням до нього випадково сформованого вектора $e = (e_0, e_1, ..., e_{n-1})$:

$$E_j = \phi_u \left(M_i, G_X^u \right) = M_i \cdot \left(G_X^u \right)^T + e , \quad (8)$$

причому вага Хеммінга (число ненульових елементів) вектора e не перевищує виправляючої можливості використаного алгебраїчного блокового коду:

$$0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor , \quad (9)$$

$\lfloor x \rfloor$ - ціла частина дійсного числа x.

Для кожного закритого сформованого тексту $E_j \in E$ вектор $e = (e_0, e_1, ..., e_{n-1})$ виступає в ролі одноразового сеансового ключа, а саме, для конкретного E_j вектор e формується випадково, рівноімовірно і незалежно від інших закритих текстів. Не знаючи правил маскування, що задається секретним ключем (набором матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$), противник змушений використовувати складний алгоритм декодування випадкового коду (в загальному випадку алгоритм експоненціальної складності) [3-5]. Навпаки, уповноважений користувач, що знає правило маскування, може скористатися швидким алгоритмом декодування алгебраїчного коду (поліноміальної складності) і відновити відкритий текст [3-5]:

$$M_i = \phi_u^{-1} \left(E_j, \{X,P,D\}_u \right). \quad (10)$$

Для відновлення відкритого тексту уповноважений користувач з прийнятого закритого тексту E_j знімає дію секретних комутативних і діагональних матриць P^u і D^u:

$$E_j^* = E_j \cdot \left(D^u \right)^{-1} \cdot \left(P^u \right)^{-1} = \left(M_i \cdot \left(G_X^u \right)^T + e \right) \cdot \left(D^u \right)^{-1} \cdot$$

$$\left(P^u \right)^{-1} = \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u \right)^T + e \right) \cdot \left(D^u \right)^{-1} \cdot \left(P^u \right)^{-1} =$$

$$= M_i \cdot \left(X^u \right)^T \cdot (G)^T \cdot \left(P^u \right)^T \cdot \left(D^u \right)^T \cdot \left(D^u \right)^{-1} \cdot \left(P^u \right)^{-1} +$$

$$+ e \cdot \left(D^u \right)^{-1} \cdot \left(P^u \right)^{-1} = M_i \cdot \left(X^u \right)^T \cdot (G)^T + e \cdot \left(D^u \right)^{-1} \cdot \left(P^u \right)^{-1},$$

декодує отриманий вектор

$$E_j^* = M_i \cdot \left(X^u \right)^T \cdot (G)^T + e \cdot \left(D^u \right)^{-1} \cdot \left(P^u \right)^{-1},$$

тобто позбавляється другого доданку і від співмножника $(G)^T$ в першому доданку в правій частині рівняння, після чого знімає дію матриці маскування X^u.

Для цього отриманий результат декодування $M_i \cdot \left(X^u \right)^T$ потрібно помножити на $\left(X^u \right)^{-1}$:

$$\left(M_i \cdot \left(X^u \right)^T \right) \cdot \left(X^u \right)^{-1} = M_i .$$

Отримане рішення – відкритий текст M_i, відповідний прийнятому закритому тексту E_j.

Вага $w(e)$ лежить в межах виправляючої можливості коду (див. вираз (9)) і є визначальною величиною при оцінці досяжного рівня безпеки і достовірності передавання даних. Так, в роботах [3-5] показано, що досяжний рівень безпеки $S_Б$ переда-

вання даних при використанні крипто-кодових засобів захисту інформації оцінюється як складність розв'язання задачі криптоаналізу найкращим (в плані обчислювальної складності) відомим не уповноваженому користувачу (порушнику) алгоритмом, точніше досяжний рівень безпеки оцінюється за критеріями мінімального ризику (оцінка в «гіршому випадку»). Задача криптоаналізу крипто-кодових засобів захисту інформації еквівалентна вирішенню задачі декодування алгебраїчного блокового (n, k, d) коду над GF(q) , замаскованого для не уповноваженого користувача (порушника) під випадковий код (код загального положення), тобто для розв'язання задачі криптоаналізу необхідно розв'язати задачу декодування кодового слова (n, k, d) коду з внесеними $w(e)$ помилками. Досяжний рівень достовірності $S_д$ передавання даних при використанні крипто-кодових засобів захисту інформації також залежить від ваги $w(e)$. Достовірність передавання даних визначається величиною $t - w(e)$, тобто максимальним числом помилок, які може виправити крипто-кодова система захисту інформації. Адаптивна зміна ваги $w(e)$ послідовностей сеансових ключів $e = (e_0, e_1, ..., e_{n-1})$ в залежності від умов застосування крипто-кодової системи захисту інформації дозволяє інтегровано забезпечувати потрібні показники безпеки і достовірності передавання даних. Проведений аналіз показав, що аналітичні вирази (1) – (10) формалізовано описують основні структурні елементи і функціональні залежності між основними компонентами секретної системи. Вихідними даними при описі несиметричної крипто-кодової системи захисту інформації з використанням алгебраїчних блокових кодів в режимі прямого виправлення помилок є:

- алгебраїчний блоковий (n, k, d) код C над GF(q), що задається своєю породжуючою матрицею G, методи і алгоритми швидкого (поліноміальної складності) кодування і декодування алгебраїчних кодів;

- маскуючі відображення, задаються множиною матриць $\{X,P,D\}_i$, обчислювальні методи і алгоритми перетворення матриць;

- методи і алгоритми формування сеансових ключів з потрібними властивостями (випадково, рівноімовірно і незалежно один від одного векторів e, які формуються).

На цей час, як показав аналіз, методи і алгоритми формування сеансових ключів у вигляді векторів e (див. вираз (8)) в доступній літературі детально не досліджували, пред'явлені потреби сформульовані в загальному вигляді і не враховують особливості побудови і функціонування інтегрованих засобів захисту інформації [1-5]. В даній роботі пропонується обчислювальний метод формування сеансових ключових даних який заснований на запропонованому в [6-8] на недвійковому рівноваговому кодуванні.

2. Недвійкове рівноважове кодування і обчислювальний метод формування сеансових ключових даних

Для формування рівноважових послідовностей на недвійковий випадок [6-8] пропонується нова форма узагальненого біноміально-позиційного представлення чисел, яка відноситься до класу змішаних систем і заснована на представленні чисел через зростаючу послідовність біноміальних коефіцієнтів, кожен з яких кодується позиційною нумерацією, тобто представлення розрядів при біноміальних коефіцієнтах засноване на помісному значенні цифр.

Розглянемо число x в запропонованій узагальненій біноміально-позиційній системі числення [6]:

$$x = \sum_{i=0}^{n-1} a_i b_i \ . \qquad (11)$$

Приймемо:

$$a_i \in \{0,1,...,q-1\}, \ b_i = \binom{u_{i+1}}{i+1} = \frac{u_{i+1}!}{(i+1)!\cdot(u_{i+1}-i-1)!},$$

$$0 \le u_1 < u_2 < ... < u_n = \frac{n!}{w!\cdot(n-w)!},$$

де w - число ненульових елементів узагальненого біноміально-позиційного коду.

Тоді число x представляється через зростаючу послідовність біноміальних коефіцієнтів $b_0, b_1, ..., b_{n-1}$ і відповідну послідовність $a_0, a_1, ..., a_{n-1}$.

Розглянемо ненульові елементи, $a_i \ne 1$, $i = 0,1,...,n-1$ послідовності $a_0, a_1, ..., a_{n-1}$ і перенумеруємо їх, тобто позначимо їх як елементи послідовності, $a_0, a_1, ..., a_{w-1}$, $l = 0,1,...,w-1$, причому, $\forall l : a_l \in \{1,...,q-1\}$. Послідовність $a_0, a_1, ..., a_{w-1}$ і всі її елементи a_l (ненульові елементи послідовності $a_0, a_1, ..., a_{n-1}$, пронумеровані в порядку зростання старшинства розрядів) утворюються з використанням позиційної системи числення за основою $q-1$, тобто $q-1$ одиниць в кожному розряді об'єднуються в одну одиницю наступного за старшинством розряду. Набір ненульових елементів, a_l, $l = 0,1,...,w-1$ задає число $x_П$, яке представляється в позиційній системі таким чином:

$$x_П = \sum_{l=0}^{w-1} (a_l - 1) h^l \ , \qquad (12)$$

де $h = q-1$ - основа використаної позиційної системи $1 \le a_l < q$.

Зростаюча послідовність біноміальних коефіцієнтів $b_0, b_1, ..., b_{n-1}$ задає число $x_Б$, яке представляється в біноміальній системі числення у вигляді:

$$x_Б = \sum_{i=0}^{n-1} a_{Бi} b_i , \qquad (13)$$

де коефіцієнти $a_{Бi} \in \{0,1\}$.

Число x в пропонованій узагальненій біноміально-позиційній системі числення задовольняє рівнянню

$$x = x_Б \cdot (q\text{-}1)^w + x_П ,$$

яке задає основне кодове обмеження на елементи узагальненого біноміально-позиційного коду.

Таким чином, використовуючи (12) і (13), число (11) у пропонованій системі узагальненого біноміально-позиційного обрахунку представляється як лінійна комбінація:

$$\begin{aligned} x &= \sum_{i=0}^{n-1} a_i b_i = x_Б \cdot (q\text{-}1)^w + x_П = \\ &= (q\text{-}1)^w \sum_{i=0}^{n-1} a_{Бi} b_i + \sum_{l=0}^{w-1} (a_l - 1)(q-1)^l \end{aligned} . \qquad (14)$$

Запропонований спосіб представлення чисел покладемо в основу методу недвійкового рівновагового кодування [7,8]. Для абстрактного визначення недвійкового рівновагового коду введемо такі формальні позначення: *n* – довжина коду; $C = \{C_0, C_1, ..., C_{M-1}\}$ – множина кодових слів, $C_j = (C_{j0} \quad C_{j1} \quad ... \quad C_{jn-1}) \in C$, $C_{ji} \in \{0,1,...,q-1\}$, $j = 0,1,...,M-1$, $i = 0,1,...,n-1$, причому $\forall j : w(C_j) = \text{const} = w$.

Потужність визначеного в такий спосіб недвійкового рівновагового коду визначається числом векторів довжини n і ваги w з елементами з множини $\{0,1,...,q-1\}$:

$$|C| = M = (q-1)^w \frac{n!}{w!(n-w)!} .$$

Недвійкове рівновагове кодування засноване на представленні інформаційних даних у вигляді числового еквіваленту A з подальшим розкладанням в лінійну комбінацію біноміальних коефіцієнтів, кожен з яких кодується позиційною нумерацією так, щоб виконувалася система кодових обмежень за довжиною рівновагових послідовностей *n*, ваги кодових слів w і потужності коду M:

$$\begin{cases} \forall j : w(C_j) = \text{const} = w; \\ 0 \le A < M; \\ 0 \le w \le n; \\ 0 \le C_{ji} < q. \end{cases}$$

Число A по правилу (14) представляється у вигляді рівновагової недвійкової послідовності $C_A = (C_{A_0} \quad C_{A_1} \quad ... \quad C_{A_{n-1}})$, причому

$$A = A_Б \cdot (q\text{-}1)^w + A_П ,$$

де $$A_Б = \sum_{i=0}^{n-1} a_{Бi} b_i , \; b_i = \binom{n-i-1}{w-1},$$

$$A_П = \sum_{l=0}^{w-1} (a_l - 1) h^l , \; h = q - 1 .$$

В роботі пропонується обчислювальний метод формування сеансових ключів для крипто-кодової системи захисту інформації в режимі прямого виправлення помилок. Він побудований на комплексному використанні прийомів і операцій недвійкового рівновагового кодування, комбінаторики, теорії чисел і структурно складається з таких етапів: запит на формування сеансового ключа із заданими параметрами (вагою $w(e)$ і довжиною n вектора $e = (e_0, e_1, ..., e_{n-1})$); розрахунок потужності L множини сеансових ключів і довжини l (в q-их символах) відповідного ненадлишкового коду:

$$L = (q-1)^{w(e)} \cdot \frac{w(e)!}{n!(n-w(e))!} , \; l = \log_q(L) ;$$

встановлення параметрів датчика послідовності випадкових чисел (довжини l і основи q); формування послідовностей довжини l випадкових (псевдовипадкових) чисел за основою q; встановлення параметрів кодера рівноваговими надлишковими кодами (довжини n і ваги $w(e)$); кодування рівноваговими надлишковими кодами (формування рівновагових послідовностей довжиною n і вагою $w(e)$); розрахунок досягнутого рівня безпеки і достовірності передавання даних.

Структура запропонованого обчислювального методу формування сеансових ключів для крипто-кодової системи захисту інформації в режимі прямого виправлення помилок представлена на рис 1.

Введений параметр $w(e)$ (потрібна вага сформованої недвійкової рівновагової послідовності) є визначаючим при оцінці безпеки і достовірності передавання даних, його адаптивна зміна залежно від умов застосування крипто-кодової системи захисту інформації дозволяє реалізувати динамічне управління для інтегрованого забезпечення потрібних показників безпеки і достовірності передавання даних.

Висновки

Таким чином, в результаті проведених досліджень здійснено подальший розвиток математичного апарату крипто-кодової системи захисту інформації з використання недвійкових рівновагових кодів для формування сеансових ключових даних і

алгебраїчних блокових кодів в режимі прямого виправлення помилок. Запропонований метод формування сеансових ключових даних реалізується з використанням розроблених процедур рівновагового недвійкового кодування і дозволяє, адаптивно міняючи вагу послідовностей, інтегровано забезпечувати потрібні показники безпеки і достовірності передавання даних у крипто-кодових системах захисту інформації в режимі прямого виправлення помилок.

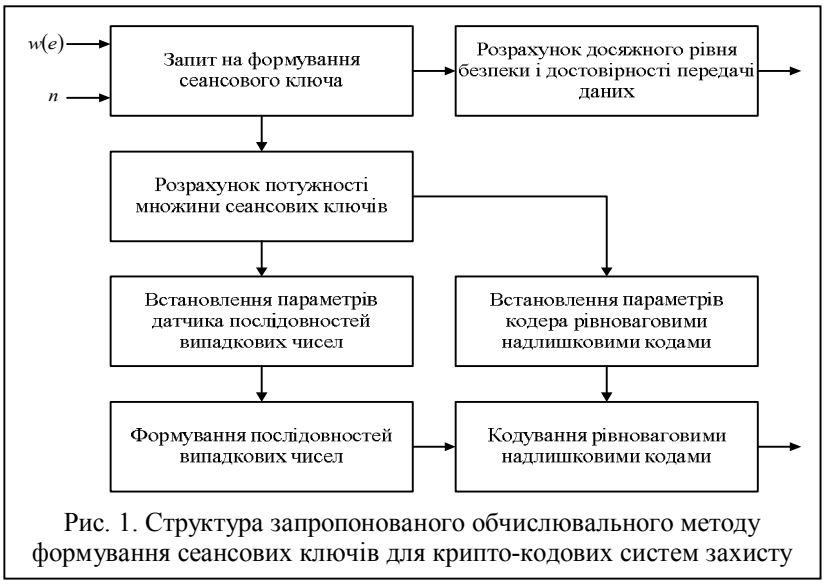

Рис. 1. Структура запропонованого обчислювального методу формування сеансових ключів для крипто-кодових систем захисту

Перспективним напрямком подальших досліджень є розробка крипто-кодових засобів захисту інформації для забезпечення потрібної безпеки і достовірності передавання даних в режимі виявлення помилок і автоматичного перезапиту, дослідження протоколів обміну конфіденційними повідомленнями з використанням відкритих ключів.

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.

6. Дудикевич В.Б. Метод недвійкового рівновагового кодування / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – №3. – С. 57 – 68.

7. Дудикевич В.Б. Крипто–кодовий захист інформації з недвійковим рівноваговим кодуванням / В.Б.Дудикевич, О.О.Кузнєцов, Б.П.Томашевський // Сучасний захист інформації. – 2010. – №2. – С. 14 – 23

8. Пат. Україна, МПК (2006.01) H 03 M 7/06. Спосіб формування рівновагових недвійкових послідовностей / заявник і власник патенту Національний університет «Львівська політехніка». – № 94308; заявка 03.08.09; опублікований 26.04.11, Бюл.№8

9. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы. - 1963. – С. 333-402.

Надійшла до редколегії 30.03.2012

Рецензент: д-р техн. наук, проф. В.Б. Дудикевич, Національний університет «Львівська політхніка», Львів.

КРИПТО-КОДОВЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА НЕДВОИЧНЫХ РАВНОВЕСНЫХ КОДАХ

Б.П. Томашевский

Рассматриваются несимметричные криптосистемы на алгебраических блоковых кодах (крипто-кодовые средства защиты информации) для построения комплексных механизмов обеспечения требуемой безопасности и достоверности передачи данных. Рассматривается формальное математическое описание несимметричных кодовых криптосистем, исследуется процесс крипто-кодового преобразования информации. На основе процедур недвоичного равновесного кодирования предлагается вычислительный метод формирования сеансовых ключевых данных, который позволяет, адаптивно изменяя вес формируемых последовательностей, интегрировано обеспечивать требуемые показатели безопасности и достоверности передачи данных в крипто-кодовых системах защиты информации.

Ключевые слова: *несимметричные криптосистемы, равновесное кодирование.*

CRYPTO-CODE SYSTEMS OF INFORMATION SECURITY WITH NONBINARY EQUILIBRIUM CODES

B.P. Tomashevskii

The article examines asymmetrical cryptosystems with algebraic block codes (crypto-code assets of information security) for constructing of integrated mechanisms in order to guarantee required level of data transmission security and reliability. It examines the formal mathematical description of asymmetrical code cryptosystems, processes of crypto-code transformation of information. It offeres the computing method to generate session key data on the basis of nonbinary equilibrium coding procedures, that allows adaptive changing of generating sequences weight, and provide required characteristics of security and reliability of data transmission in crypto-code systems of information security.

Keywords: *asymmetrical cryptosystems, equilibrium encryption.*