УДК 511.216

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 306-313

АНАЛІТИЧНІ ЗАЛЕЖНОСТІ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ ЕЛЕМЕНТІВ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ МОЖЛИВОСТІ ПОБУДОВИ МЕТОДІВ АВТЕНТИФІКАЦІЇ ТА ЦИФРОВОГО ПІДПИСУВАННЯ

Ю.Є. Яремчук

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: yurevyar@vntu.net

Проведено дослідження рекурентних V_k –послідовностей та отримано аналітичні залежності прискореного обчислення елементів цієї послідовності. Встановлено властивості обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$. Це дозволило розширити математичний апарат рекурентних V_k –послідовностей щодо можливості побудови асиметричних криптографічних методів різного призначення, зокрема методів автентифікації та цифрового підписування.

Ключові слова: рекурентні послідовності, аналітичні залежності, криптографія, автентифікація, цифрове підписування

Вступ

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [1]:

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k},$$

де

$a_1, a_2, \ldots, a_k$ — коефіцієнти,

k — порядок послідовності, виходячи з початкових елементів $u_0, u_1, \ldots, u_k$.

Прикладом рекурентної послідовності є відома послідовність Фібоначчі [2], для якої

$$u_n = u_{n-1} + u_{n-2},$$

з початковими елементами $u_0 = 1$ та $u_1 = 1$.

В [3] розглянуто математичний апарат рекурентних V_k – та U_k –послідовностей, в яких початкові елементи пов’язані з коефіцієнтами рекурентного співвідношення. Використовуючи цей апарат, було запропоновано методи асиметричного шифрування інформації, які забезпечили прискорення обчислень у порівнянні з відомими аналогами.

В [3] було запропоновано ідею використання математичного апарату рекурентних V_k– та U_k–послідовностей для побудови асиметричних криптографічних методів різного призначення, як то розподілу секретних ключів, автентифікації та цифрового підписування. Для цього отримано аналітичні залежності для V_k–послідовності, що забезпечують можливість прискореного обчислення елементів $v_{n+m,k}$ та $v_{n-m,k}$ цієї послідовності для цілих додатних n, m та k. На основі цих залежностей в [3] було представлено методи асиметричного шифрування інформації, що базуються на V_k– та U_k–послідовностях.

Однак, для побудови асиметричних криптографічних методів автентифікації сторін взаємодії та цифрового підписування отриманих залежностей недостатньо, оскільки ці криптографічні призначення використовують більш складні криптографічні перетворення, ніж при шифруванні. Тому для розширення можливості побудови асиметричних криптографічних методів різного призначення виникає необхідність отримання аналітичних залежностей прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$.

Мета роботи

Дослідження рекурентних V_k–послідовностей щодо отримання аналітичних залежностей прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$.

Постановка задач досліджень

Розглянути математичний апарат рекурентних V_k–послідовностей, встановити і довести аналітичні залежності прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$ для цієї послідовності.

Дослідження можливості отримання аналітичних залежностей прискореного обчислення елементів $v_{-n+m,k}$ та $v_{-n-m,k}$ для V_k–послідовності

V_k–послідовність [3] складається з V_k^+– та V_k^-–послідовності.

V_k^+–послідовність визначається як послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot v_{n-k,k} \qquad (1)$$

при початкових значеннях $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k — цілі числа; n і k — цілі додатні числа.

Формула (1) дозволяє отримувати елементи послідовності для зростаючих n, починаючи з $n = 0$. Зворотна процедура обчислення елементів послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (2)$$

Формула (2) дозволяє обчислювати елементи V_k^+ –послідовності, тобто елементи $v_{n,k}$ з додатними значеннями індексу для спадних n. Обчислення за формулою (2) може продовжуватись і для від'ємних значень індексу. В такому випадку обчислення елементів $v_{-n,k}$, теж для спадних n, буде здійснюватись за такою формулою

$$v_{-n,k} = \frac{v_{-n+k,k} - g_k \cdot v_{-n+k-1,k}}{g_1}. \qquad (3)$$

Тобто існує два виду послідовностей: перший вид послідовності формується для додатних значень індексу, тобто елементів $v_{n,k}$, за формулою (1); другий вид послідовності формується для від'ємних значень індексу, тобто елементів $v_{-n,k}$, за формулою (3).

Другий вид послідовності – це V_k^- –послідовність, яку визначимо як послідовність чисел, що обчислюються за формулою (3) для від'ємних значень індексів, тобто елементів $v_{-n,k}$, де n і k – цілі додатні числа, при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Тоді формула (1), яка дозволяє обчислювати елементи $v_{n,k}$ послідовності V_k^+ з додатними значеннями індексу для зростаючих n, для обчислення елементів $v_{-n,k}$ послідовності V_k^- з від'ємними значеннями індексу, теж для зростаючих n, буде мати такий вигляд

$$v_{-n,k} = g_k \cdot v_{-n-1,k} + g_1 \cdot v_{-n-k,k}. \qquad (4)$$

Теорема 1. Для будь-яких цілих додатних n, m та k

$$v_{-n+m,k} = v_{m+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{-n-k+i,k}. \qquad (5)$$

Доведення. Проведемо доведення аналітичної залежності (5) індукцією по m.

Оскільки V_k^+ –послідовність приймає різні початкові значення для $k = 2$ та $k > 2$, тому основу індукції доведемо окремо для обох цих випадків.

Спочатку доведемо основу індукції для $k = 2$.

В такому випадку аналітична залежність (5) буде мати вигляд

$$v_{-n+m,2} = v_{m,2} \cdot v_{-n,2} + g_1 \cdot v_{m-1,k} \cdot v_{-n-1,k}, \qquad (6)$$

а формула (4) запишіться як $v_{-n,2} = g_2 \cdot v_{-n-1,2} + g_1 \cdot v_{-n-2,2}$.

Покажемо, що (6) виконується для m, що дорівнюють 1 і 2.

$$v_{-n+1,2} = v_{1,2} v_{-n,2} + g_1 v_{0,k} v_{-n-1,2} = g_2 v_{-n,2} + g_1 v_{-n-1,2} = g_2 v_{(-n-1)+1,2} + g_1 v_{(-n-2)-1,2} = v_{-n+1,2}.$$

$$v_{-n+2,2} = v_{2,2}v_{-n,2} + g_1 v_{1,k} v_{-n-1,2}.$$

З (1) $v_{2,2} = g_2 v_{1,2} + g_1 v_{0,2} = g_2^2 + g_1$. Враховуючи це,

$$v_{-n+2,2} = \left(g_2^2 + g_1\right)v_{-n,2} + g_1 g_2 v_{-n-1,2} = g_2^2 v_{-n,2} + g_1 v_{-n,2} + g_1 g_2 v_{-n-1,2} =$$

$$= g_2\left(g_2 v_{-n,2} + g_1 v_{-n-1,2}\right) + g_1 v_{-n,2} = g_2 v_{-n+1,2} + g_1 v_{-n,2} = g_2 v_{(-n-1)+2,2} + g_1 v_{(-n-2)+2,2} = v_{-n+2,2}.$$

Таким чином, основу індукції для $k = 2$ доведено.

Доведемо тепер основу індукції для $k > 2$.

Покажемо, що (5) виконується для m, які дорівнюють 1, 2 , 3, . . . , k

$$v_{-n+1,k} = v_{k-1,k}v_{-n,k} + g_1 v_{k-2,k} v_{-n-k+1,k} + g_1 v_{k-3,k} v_{-n-k+2,k} + \ldots + g_1 v_{0,k} v_{-n-1,k}.$$

Враховуючи значення початкових елементів V_k^+–послідовності, отримаємо $v_{-n+1,k} = g_k v_{-n,k} + g_1 v_{-n-k+1,k}$.

Якщо записати це як $v_{(-n)+1,k} = g_k v_{(-n-1)+1,k} + g_1 v_{(-n-k)+1,k}$, то з (4) видно, що аналітична залежність (5) виконується для $m = 1$.

Аналогічно знайдемо тепер $v_{-n+2,k}$.

$$v_{-n+2,k} = v_{k,k}v_{-n,k} + g_1 v_{k-1,k} v_{-n-k+1,k} + g_1 v_{k-2,k} v_{-n-k+2,k} + g_1 v_{k-3,k} v_{-n-k+3,k} + \ldots + g_1 v_{1,k} v_{-n-1,k}.$$

Виходячи з (1), $v_{k,k} = g_k v_{k-1,k} + g_1 v_{0,k} = g_k v_{k-1,k}$. Враховуючи це, а також значення початкових елементів V_k^+–послідовності, отримаємо

$$v_{-n+2,k} = g_k v_{k-1,k} v_{-n,k} + g_1 v_{k-1,k} v_{-n-k+1,k} + g_1 v_{k-2,k} v_{-n-k+2,k} =$$

$$= v_{k-1,k}\left(g_k v_{-n,k} + g_1 v_{-n-k+1,k}\right) + g_1 v_{-n-k+2,k} =$$

$$= g_k v_{-n+1,k} + g_1 v_{-n-k+2,k} = g_k v_{(-n-1)+2,k} + g_1 v_{(-n-k)+2,k}.$$

Враховуючи (4), переконуємось, що останній вираз дорівнює $v_{-n+2,k}$, тобто аналітична залежність (5) виконується і для $m = 2$.

Роблячи таким же чином, знайдемо $v_{-n+3,k}$.

$$v_{-n+3,k} = v_{k+1,k} v_{-n,k} + g_1 v_{k,k} v_{-n-k+1,k} + g_1 v_{k-1,k} v_{-n-k+2,k} + g_1 v_{k-2,k} v_{-n-k+3,k} +$$

$$+ g_1 v_{k-3,k} v_{-n-k+4,k} + \ldots + g_1 v_{2,k} v_{-n-1,k} =$$

$$= \left(g_k v_{k,k} + g_1 v_{1,k}\right)v_{-n,k} + g_1 v_{k,k} v_{-n-k+1,k} + g_1 v_{k-1,k} v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= v_{k,k}\left(g_k v_{-n,k} + g_1 v_{-n-k+1,k}\right) + g_1 v_{k-1,k} v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= v_{k,k} v_{-n+1,k} + g_1 v_{k-1,k} v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= \left(g_k v_{k-1,k} + g_1 v_{0,k}\right) v_{-n+1,k} + g_1 v_{k-1,k} v_{-n-k+2,k} + g_1 v_{-n-k+3,k} =$$

$$= v_{k-1,k}\left(g_k v_{-n+1,k} + g_1 v_{-n-k+2,k}\right) + g_1 v_{-n-k+3,k} =$$

$$= g_k v_{-n+2,k} + g_1 v_{-n-k+3,k} = g_k v_{(-n-1)+3,k} + g_1 v_{(-n-k)+3,k} = v_{-n+3,k}$$

. . .

$$v_{-n+k,k} = v_{2k-2,k} v_{-n,k} + g_1 v_{2k-3,k} v_{-n-k+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= \left(g_k v_{2k-3,k} + g_1 v_{k-2,k}\right) v_{-n,k} + g_1 v_{2k-3,k} v_{-n-k+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-3,k}\left(g_k v_{-n,k} + g_1 v_{-n-k+1,k}\right) + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-3,k} v_{-n+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} + g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= \left(g_k v_{2k-4,k} + g_1 v_{k-3,k}\right) v_{-n+1,k} + g_1 v_{2k-4,k} v_{-n-k+2,k} +$$

$$+ g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-4,k}\left(g_k v_{-n+1,k} + g_1 v_{-n-k+2,k}\right) + g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_1 v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} =$$

$$= v_{2k-4,k} v_{-n+2,k} + g_1 v_{2k-5,k} v_{-n-k+3,k} + \ldots + g_{1,k} v_{k,k} v_{-n-2,k} + g_1 v_{k-1,k} v_{-n-1,k} = \ldots =$$

$$= v_{k-1,k} v_{-n+k-1,k} + g_1 v_{k-2,k} v_{-n,k} = g_k v_{-n+k-1,k} + g_1 v_{-n,k} .$$

Таким чином основу індукції для $k > 2$ доведено.

Нехай аналітична залежність (5) виконується для $m-k$, $m-k+1$, . . . , $m-1$. Покажемо, що вона виконується для m.

$$v_{-n+m,k} = g_k v_{-n+m-1,k} + g_1 v_{-n+m-k,k} =$$

$$= g_k v_{m-1+(k-2),k} v_{-n,k} + g_1 g_k \sum_{i=1}^{k-1} v_{m-1+(k-2)-i,k} v_{-n-k+i,k} +$$

$$+ g_1 v_{m-k+(k-2),k} v_{-n,k} + g_1^2 \sum_{i=1}^{k-1} v_{m-k+(k-2)-i,k} v_{-n-k+i,k} =$$

$$= g_k v_{m-1+(k-2),k} v_{-n,k} + g_1 g_k v_{m-1+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1 g_k v_{m-1+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 g_k v_{m-1+(k-2)-(k-1),k} v_{-n-1,k} +$$

$$+ g_1 v_{m-k+(k-2),k} v_{-n,k} + g_1^2 v_{m-k+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1^2 v_{m-k+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1^2 v_{m-k+(k-2)-(k-1),k} v_{-n-1,k} =$$

$$= \left(g_k v_{m-1+(k-2),k} + g_1 v_{m-k+(k-2),k}\right) v_{-n,k} + g_1 \left(g_k v_{m-1+(k-2)-1,k} + g_1 v_{m-k+(k-2)-1,k}\right) v_{-n-k+1,k} +$$

$$+ g_1 \left(g_k v_{m-1+(k-2)-2,k} + g_1 v_{m-k+(k-2)-2,k}\right) v_{-n-k+2,k} + \ldots +$$

$$+ g_1 \left(g_k v_{m-1+(k-2)-(k-1),k} + g_1 v_{m-k+(k-2)-(k-1),k}\right) v_{-n-1,k} =$$

$$= v_{m+(k-2),k} v_{-n,k} + g_1 v_{m+(k-2)-1,k} v_{-n-k+1,k} + g_1 v_{m+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 v_{m+(k-2)-(k-1),k} v_{-n-1,k} =$$

$$= v_{m+(k-2),k} v_{-n,k} + g_1 \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} v_{-n-k+i,k} .$$

Теорему доведено.

Теорема 2. Для будь-яких цілих додатних n, m та k

$$v_{-n-m,k} = v_{-m+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{-n-k+i,k} . \qquad (7)$$

Доведення. Проведемо доведення аналітичної залежності (7) індукцією по m. Покажемо, що (7) виконується для m, які дорівнюють 1, 2 , 3, . . . , k.

$$v_{-n-1,k} = v_{k-3,k} v_{-n,k} + g_1 v_{k-4,k} v_{-n-k+1,k} + \ldots + g_1 v_{-1,k} v_{-n-2,k} + g_1 v_{-2,k} v_{-n-1,k} .$$

Враховуючи значення початкових елементів, отримаємо

$$v_{-n-1,k} = g_1 g_1^{-1} v_{-n-1,k} = v_{-n-1,k} .$$

Знайдемо тепер $v_{-n-2,k}$

$$v_{-n-2,k} = v_{k-4,k} v_{-n,k} + g_1 v_{k-5,k} v_{-n-k+1,k} + \ldots +$$

$$+ g_1 v_{-1,k} v_{-n-3,k} + g_1 v_{-2,k} v_{-n-2,k} + g_1 v_{-3,k} v_{-n-1,k} = g_1 v_{-2,k} v_{-n-2,k} = v_{-n-2,k}$$

. . .

$$v_{-n-k,k} = v_{-2,k} v_{-n,k} + g_1 v_{-3,k} v_{-n-k+1,k} + \ldots + g_1 v_{-k,k} v_{-n-2,k} + g_1 v_{-k-1,k} v_{-n-1,k} =$$

$$= v_{-2,k} v_{-n,k} + g_1 v_{-k-1,k} v_{-n-1,k} = g_1^{-1} v_{-n,k} + g_1 \left(- g_k g_1^{-2}\right) v_{-n-1,k} = \frac{v_{-n,k} - g_k v_{-n-1,k}}{g_1} = v_{-n-k,k} .$$

Нехай залежність (7) виконується для $m+1$, $m+2$, . . . , $m+k$. Покажемо, що вона виконується для m.

$$v_{-n-m,k} = g_k v_{-n-m-1,k} + g_1 v_{-n-m-k,k} =$$

$$= g_k v_{-m-1+(k-2),k} v_{-n,k} + g_1 g_k \sum_{i=1}^{k-1} v_{-m-1+(k-2)-i,k} v_{-n-k+i,k} +$$

$$+ g_1 v_{-m-k+(k-2),k} v_{-n,k} + g_1^2 \sum_{i=1}^{k-1} v_{-m-k+(k-2)-i,k} v_{-n-k+i,k} =$$

$$= g_k v_{-m-1+(k-2),k} v_{-n,k} + g_1 g_k v_{-m-1+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1 g_k v_{-m-1+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 g_k v_{-m-1+(k-2)-(k-1),k} v_{-n-1,k} +$$

$$+ g_1 v_{-m-k+(k-2),k} v_{-n,k} + g_1^2 v_{-m-k+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1^2 v_{-m-k+(k-2)-1,k} v_{-n-k+1,k} + \ldots + g_1^2 v_{-m-k-1,k} v_{-n-1,k} =$$

$$= \left(g_k v_{-m-1+(k-2),k} + g_1 v_{-m-k+(k-2),k}\right) v_{-n,k} +$$

$$+ g_1 \left(g_k v_{-m-1+(k-2)-1,k} + g_1 v_{-m-k+(k-2)-1,k}\right) v_{-n-k+1,k} +$$

$$+ g_1 \left(g_k v_{-m-1+(k-2)-2,k} + g_1 v_{-m-k+(k-2)-2,k}\right) v_{-n-k+2,k} + \ldots +$$

$$+ g_1 \left(g_k v_{-m-1+(k-2)-(k-1),k} + g_1 v_{-m-k+(k-2)-(k-1),k}\right) v_{-n-1,k} =$$

$$= v_{-m+(k-2),k} v_{-n,k} + g_1 v_{-m+(k-2)-1,k} v_{-n-k+1,k} +$$

$$+ g_1 v_{-m+(k-2)-2,k} v_{-n-k+2,k} + \ldots + g_1 v_{-m+(k-2)-(k-1),k} v_{-n-1,k} =$$

$$= v_{-m+(k-2),k} v_{-n,k} + g_1 \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} v_{-n-k+i,k} \,.$$

Це і вимагалося довести.

В окремому випадку, коли $m = n$ аналітична залежність (7) буде мати такий вигляд

$$v_{-2n,k} = v_{-n+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-n+(k-2)-i,k} \cdot v_{-n-k+i,k} \,. \qquad (8)$$

Висновки

Проведено дослідження рекурентної V_k–послідовності, що складається з двох послідовностей V_k^+ і V_k^-. Отримано властивості, що дозволяють здійснювати прискорене обчислення елементів цієї послідовності, а саме елементів $v_{-n+m,k}$ та $v_{-n-m,k}$.

Отримані властивості дозволили розширити математичний апарат рекурентних V_k –послідовностей щодо можливості побудови асиметричних криптографічних методів різного призначення, зокрема методів автентифікації та цифрового підписування.

Список літератури

1. Маркушевич, А.И. Возвратные последовательности [Текст] : научно-популярная литература / А.И. Маркушевич. — 3-е изд. — М. : Физ.-мат. лит.: Наука, 1983. — 48 с.
2. Воробьев, Н.Н. Числа Фибоначчи [Текст] / Н.Н. Воробьев. — 6-е изд., доп. — М. : Наука, 1992. — 192 с.
3. Яремчук, Ю.Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей [Текст] : монографія / Ю.Є. Яремчук. — Вінниця : Книга-Вега, 2002. — 136 с.

АНАЛИТИЧЕСКИЕ ЗАВИСИМОСТИ УСКОРЕННОГО ВЫЧИСЛЕНИЯ ЭЛЕМЕНТОВ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ВОЗМОЖНОСТИ ПОСТРОЕНИЯ МЕТОДОВ АУТЕНТИФИКАЦИИ И ЦИФРОВОГО ПОДПИСЫВАНИЯ

Ю.Е. Яремчук

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

Проведено исследование рекуррентных V_k –последовательностей и получены аналитические зависимости ускоренного вычисления элементов этой последовательности. Установлены свойства вычисления элементов $v_{-n+m,k}$ и $v_{-n-m,k}$. Это позволило расширить математический аппарат рекуррентных V_k –последовательностей для возможности построения асимметричных криптографических методов различного назначения, в частности методов аутентификации и цифрового подписания.

Ключевые слова: рекуррентные последовательности, аналитические зависимости, криптография, аутентификация, цифровое подписание

ANALYTIC DEPENDENCES OF FAST COMPUTATION OF THE TERMS OF RECURRENT SEQUENCES TO BE USED IN THE DEVELOPMENT OF AUTHENTICATION AND DIGITAL SIGNATURE TECHNIQUES

Yuri E. Yaremchuk

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

Recurrent V_k sequences were investigated and analytic dependences related to fast computation of the terms of such a sequence obtained. The features of computation of $v_{-n+m,k}$ and $v_{-n-m,k}$ terms were established. This made it possible to expand the mathematical apparatus for recurrent V_k sequences that may be used to develop asymmetric cryptographic techniques of various purposes, including authentication and digital signature techniques.

Keywords: recurrent sequences, analytical dependences, cryptography, authentication, digital signature