2. Chrysostomou C., Pitsillides A., Hadjipollas G., Polycarpou M., Sekercioglu A."Fuzzy Logic Congestion Control in TCP/IP Best-effort Networks", Australian Telecommunications Networks and Applications Conference (Atnac 2003), Melbourne, Australia, 8–10 December 2003.

3. Liu Weiyan, Zhang Shunyi, Zhang Mu, Liu Tao. "A Fuzzy-Logic Control Algorithm for Active Queue Management in IP Networks". - Journal of Electronics (China), Vol.25, No.1, January 2008.

4. Гостев В.И. Нечеткие регуляторы в системах автоматического управления / В.И. Гостев. – К.: Издательство "Радіоаматор", 2008. – 972 с.

5. Гостев В.И. Проектирование нечетких регуляторов для систем автоматического управления / В.И. Гостев. – Спб.: Бхв-Петербург, 2011. – 416 с.

УДК 511.216

Яремчук Ю.Є., *к.т.н.* (*Вінницький національний технічний університет*)

МАТЕМАТИЧНИЙ АПАРАТ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПОБУДОВИ КРИПТОГРАФІЧНИХ МЕТОДІВ З ВІДКРИТИМ КЛЮЧЕМ

Яремчук Ю.Є. Математичний апарат рекурентних послідовностей для побудови криптографічних методів з відкритим ключем. В роботі розглянуто рекурентну U_k-послідовність, для якої встановлено аналітичні залежності безпосереднього обчислення елементу послідовності, а також обчислення елементів U_k-послідовності тільки на основі елементів V_k^+-послідовності. Створений математичний апарат може стати основою для побудови криптографічних методів з відкритим ключем.

Ключові слова: КРИПТОГРАФІЯ, МАТЕМАТИЧНИЙ АПАРАТ, РЕКУРЕНТНА ПОСЛІДОВНІСТЬ, V_k^+-ПОСЛІДОВНІСТЬ,, V_k^--ПОСЛІДОВНІСТЬ

Яремчук Ю.Е. Математический аппарат рекуррентных последовательностей для построения криптографических методов с открытым ключом. В работе рассмотрено рекуррентную U_k-последовательность, для которой установлены аналитические зависимости непосредственного вычисления элемента последовательности, а также вычисления элементов U_k-последовательности только на основе элементов V_k^+ - последовательности. Созданный математический аппарат может стать основой для построения криптографических методов с открытым ключом.

Ключевые слова: КРИПТОГРАФИЯ, МАТЕМАТИЧЕСКИЙ АППАРАТ, РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k^+-ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k^--ПОСЛЕДОВАТЕЛЬНОСТЬ,

Iaremchuk Iu.Ie. Mathematical apparatus of recurrent sequences for constructing cryptographic techniques with public key. We consider recursive U_k-sequence for which an analytical dependence of direct computation element sequences and computing elements U_k-order only on the basis of elements V_k^+-sequence. Created mathematical tools can be the basis for the construction of cryptographic techniques with public key.

Keywords: CRYPTOGRAPHY, MATHEMATICAL APPARATUS, RECURRENT SEQUENCE, V_k^+-SEQUENCE, V_k^--SEQUENCE

Вступ. Рекурентні послідовності в загальному вигляді породжується таким співвідношенням $u_n = a_1 u_{n-1} + a_2 u_{n-2} + ... + a_k u_{n-k}$, де $a_1, a_2, ..., \tilde{a}_k$ коефіцієнти, $\tilde{k}$ порядок послідовності, виходячи з початкових елементів $u_0, u_1, ..., u_k$ [1].

Складність обчислення елементів такої послідовності залежить від кількості ненульових коефіцієнтів $a_1, a_2, ..., a_k$ та від порядку k рекурентного співвідношення.

Відомими прикладами вказаної послідовності є послідовність Фібоначчі [2] та послідовність Хорадама [3, 4]. В усіх цих послідовностях початкові елементи – довільні числа, які не пов'язані з коефіцієнтами.

Певну цікавість представляють послідовності, в яких початкові елементи пов'язані з коефіцієнтами. Найпростішим прикладом в цьому випадку є послідовність, елементи якої обчислюються за формулою $u_n = a_1 u_{n-1}$. Якщо $u_1 = q$, $a_1 = q$, то $u_n = q^n$. Тобто, в цьому випадку, рекурентне співвідношення породжує степеневу послідовність.

Наступним за складністю є випадок, коли два коефіцієнти відрізняються від нуля. В цьому випадку елементи послідовності обчислюються за формулою $u_n = a_1 u_{n-1} + a_k u_{n-k}$.

Актуальним стає питання дослідження таких послідовностей, а також більш узагальнених послідовностей, в яких початкові елементи пов'язані з коефіцієнтами, оскільки такі послідовності, а також отримані для них аналітичні залежності можуть стати основою для побудови криптографічних методів з відкритим ключем.

Математичні апарат рекурентних U_k-послідовностей для побудови криптографічних методів. Назвемо U_k-послідовністю послідовність чисел, що обчислюються за формулою

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

при початкових значеннях $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ... $u_{k-1,k} = g_k$, де $g_1, g_2, g_3, ..., g_k$ – цілі числа; n і k – цілі додатні числа.

Покажемо перші $2k-1$ елементів послідовності.

$u_{k+2,k}$	$u_{k+1,k}$	$u_{k,k}$	$u_{k-1,k}$	. . .	$u_{1,k}$	$u_{0,k}$
$g_k^4 + g_1^2 g_k^2 + g_1 g_2 g_k + g_1 g_3$	$g_k^3 + g_1^2 g_k + g_1 g_2$	$g_k^2 + g_1^2$	g_k	. . .	g_2	g_1

. . .	$u_{2k-1,k}$	. . .	$u_{k+3,k}$
. . .	$g_k^{k+1} + g_1 g_1 g_k^{k-1} + g_1 g_2 g_k^{k-2} + g_1 g_3 g_k^{k-3} + ... + g_1 g_{k-1} g_k^{k-(k-1)} + g_1 g_k$	. . .	$g_k^5 + g_1^2 g_k^3 + g_1 g_2 g_k^2 + g_1 g_3 g_k + g_1 g_4$

Виходячи з формули (1) залежність для обчислення елементів для спадних n, починаючи з деякого $n = l$, буде мати такий вигляд

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

Окремим випадком U_k-послідовності є V_k^+-послідовність, елементи якої обчислюються за формулою

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

при початкових значеннях $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$.

Важливою характеристикою оцінювання криптографічних методів є їх криптографічна стійкість. В цьому зв'язку, в разі побудови криптографічних методів на основі $\tilde{U_k}$-послідовності, важливим є отримання залежності безпосереднього обчислення елементу $u_{n,k}$ через початкові елементи.

Для будь-яких цілих додатних n і k, таких що $n \geq k$ отримано таку залежність

$$u_{n,k} = g_k^{n-(k-2)} + \sum_{i=1}^{\left\lfloor \frac{n}{k} \right\rfloor} g_k^{n-(k-2)-ki} \cdot g_1^i \left(\sum_{j=1}^{k-1} C_{n-(k-1)i-j}^{i-1} \cdot g_k^{k-j-1} \cdot g_j + C_{n-(k-1)-(k-1)i}^{i} \right). \qquad \textbf{(4)}$$

Проведемо аналіз цієї залежності індукцією по n.

Покажемо, що (4) виконується для n, які дорівнюють k, $k+1$, $k+2$, $k+3, ..., 2k-1$.

$$u_{k,k} = g_k^2 + C_0^0 g_1^2 + C_{-1}^0 g_1 g_2 g_k^{-1} + ... = g_k^2 + g_1^2,$$

$$u_{k+1,k} = g_k^3 + C_1^0 g_1 g_1 g_k + C_0^0 g_1 g_2 + C_{-1}^0 g_1 g_3 g_k^{-1} + ... = g_k^3 + g_1 g_1 g_k + g_1 g_2,$$

$$u_{k+2,k} = g_k^4 + C_2^0 g_1 g_1 g_k^2 + C_1^0 g_1 g_2 g_k + C_0^0 g_1 g_3 + C_{-1}^0 g_1 g_4 g_k^{-1} + ... = g_k^4 + g_1 g_1 g_k^2 + g_1 g_2 g_k + g_1 g_3,,$$

$$u_{k+3,k} = g_k^5 + C_3^0 g_1 g_1 g_k^3 + C_2^0 g_1 g_2 g_k^2 + C_1^0 g_1 g_3 g_k + C_0^0 g_1 g_4 + C_{-1}^0 g_1 g_5 g_k^{-1} + ... =$$

$$= g_k^5 + g_1 g_1 g_k^3 + g_1 g_2 g_k^2 + g_1 g_3 g_k + g_1 g_4, ...$$

$$u_{2k-1,k} = g_k^{k+1} + C_{k-1}^0 g_1 g_1 g_k^{k-1} + C_{k-2}^0 g_1 g_2 g_k^{k-2} + C_{k-3}^0 g_1 g_3 g_k^{k-3} + ... +$$

$$+ C_1^0 g_1 g_{k-1} g_k + C_1^1 g_k g_1 = g_k^{k+1} + g_1 g_1 g_k^{k-1} + g_1 g_2 g_k^{k-2} + g_1 g_3 g_k^{k-3} + ... + g_1 g_{k-1} g_k + g_1 g_k.$$

Основа індукції, таким чином, доведена.

Нехай залежність (4) виконується для $n-k, n-k+1, ..., n-1$. Покажемо, що вона виконується для n.

$$u_{n,k} = g_k \cdot u_{n-1,k} + g_1 \cdot u_{n-k,k} = g_k^{n-(k-2)} + \sum_{i=1}^{\left|\frac{n-1}{k}\right|} g_k^{n-(k-2)-ki} \cdot g_1^i \cdot (\sum_{j=1}^{k-1} C_{n-1-(k-1)i-j}^{i-1} \cdot g_k^{k-j-1} \cdot g_j + C_{n-1-(k-1)-(k-1)i}^{i}) +$$

$$+ g_k^{n-k-(k-2)} \cdot g_1 + \sum_{i=1}^{\left|\frac{n-k}{k}\right|} g_k^{n-k-(k-2)-ki} \cdot g_1^{i+1} \cdot (\sum_{j=1}^{k-1} C_{n-k-(k-1)i-j}^{i-1} \cdot g_k^{k-j-1} \cdot g_j + C_{n-k-(k-1)-(k-1)i}^{i}) =$$

$$= g_k^{n-(k-2)} + C_{n-k-1}^0 g_k^{n-k} g_1^2 + C_{n-k-2}^0 g_k^{n-k-1} g_1 g_2 + C_{n-k-3}^0 g_k^{n-k-2} g_1 g_3 + ... + C_{n-2k+1}^0 g_k^{n-2k+2} g_1 g_{k-1} +$$

$$+ C_{n-2k+1}^1 g_k^{n-2k+2} g_1 + C_{n-2k}^1 g_k^{n-2k} g_1^3 + C_{n-2k-1}^1 g_k^{n-2k-1} g_1^2 g_2 + C_{n-2k-2}^1 g_k^{n-2k-2} g_1^2 g_3 + ... +$$

$$+ C_{n-3k+2}^1 g_k^{n-3k+2} g_1^2 g_{k-1} + C_{n-3k+2}^2 g_k^{n-3k+2} g_1^2 + C_{n-3k+1}^2 g_k^{n-3k} g_1^4 + C_{n-3k}^2 g_k^{n-3k-1} g_1^3 g_2 + C_{n-3k-1}^2 g_k^{n-3k-2} g_1^3 g_3 +$$

$$+ ... + C_{n-4k+3}^2 g_k^{n-4k+2} g_1^3 g_{k-1} + C_{n-4k+3}^3 g_k^{n-4k+2} g_1^3 + ... +,,_{n-2k+1}^0 g_k^{n-2k+2} g_1 + C_{n-2k}^0 g_k^{n-2k} g_1^3 +$$

$$+ C_{n-2k-1}^0 g_k^{n-2k-1} g_1^2 g_2 + C_{n-2k-2}^0 g_k^{n-2k-2} g_1^2 g_3 + ... + C_{n-3k+2}^0 g_k^{n-3k+2} g_1^2 g_{k-1} + C_{n-3k+2}^1 g_k^{n-3k+2} g_1^2 +$$

$$+ C_{n-3k+1}^1 g_k^{n-3k} g_1^4 + C_{n-3k}^1 g_k^{n-3k-1} g_1^3 g_2 + C_{n-3k-1}^1 g_k^{n-3k-2} g_1^3 g_3 + ... + C_{n-4k+3}^1 g_k^{n-4k+2} g_1^3 g_{k-1} + C_{n-4k+3}^2 g_k^{n-4k+2} g_1^3 +$$

$$+ C_{n-4k+2}^2 g_k^{n-4k} g_1^5 + C_{n-4k+1}^2 g_k^{n-4k-1} g_1^4 g_2 + C_{n-4k}^2 g_k^{n-4k-2} g_1^4 g_3 + ... + C_{n-5k+4}^2 g_k^{n-5k+2} g_1^4 g_{k-1} + C_{n-5k+4}^3 g_k^{n-5k+2} g_1^4 + ...$$

Тут доданок $g_k^{n-2k+2} g_1$ добавлений C_{n-2k+1}^0, оскільки для будь-якого m $C_m^0 = 1$. Відомо [5], що

$$C_n^r + C_n^{r+1} = C_{n+1}^{r+1}, \qquad \textbf{(5)}$$

і для будь-яких n та m $C_n^0 = C_m^0$.

Враховуючи це та замінюючи доданки попарно з урахуванням (5), отримаємо :

$$u_{n,k} = g_k^{n-(k-2)} + C_{n-k}^0 g_k^{n-k} g_1^2 + C_{n-k-1}^0 g_k^{n-k-1} g_1 g_2 + C_{n-k-2}^0 g_k^{n-k-2} g_1 g_3 + ... + C_{n-2k+2}^0 g_k^{n-2k+2} g_1 g_{k-1} + C_{n-2k+2}^1 g_k^{n-2k+2} g_1 +$$

$$+ C_{n-2k+1}^1 g_k^{n-2k} g_1^3 + C_{n-2k}^1 g_k^{n-2k-1} g_1^2 g_2 + C_{n-2k-1}^1 g_k^{n-2k-2} g_1^2 g_3 + ... + C_{n-3k+3}^1 g_k^{n-3k+2} g_1^2 g_{k-1} + C_{n-3k+3}^2 g_k^{n-3k+2} g_1^2 +$$

$$+ C_{n-3k+2}^2 g_k^{n-3k} g_1^4 + C_{n-3k+1}^2 g_k^{n-3k+1} g_1^3 g_2 + C_{n-3k}^2 g_k^{n-3k-2} g_1^3 g_3 + ... + C_{n-4k+4}^2 g_k^{n-4k+2} g_1^3 g_{k-1} + C_{n-4k+4}^3 g_k^{n-4k+2} g_1^3 + ...$$

Представимо тепер залежність (4), розписавши в ній суми.

$$u_{n,k} = g_k^{n-(k-2)} + g_k^{n-(k-2)-k} \cdot g_1 (\sum_{j=1}^{k-1} C_{n-(k-1)-j}^0 \cdot g_k^{k-j-1} \cdot g_j + C_{n-(k-1)-(k-1)}^1) +$$

$$+ g_k^{n-(k-2)-2k} \cdot g_1^2 (\sum_{j=1}^{k-1} C_{n-2(k-1)-j}^1 \cdot g_k^{k-j-1} \cdot g_j + C_{n-(k-1)-2(k-1)}^2) +$$

$$+ g_k^{n-(k-2)-3k} \cdot g_1^3 (\sum_{j=1}^{k-1} C_{n-3(k-1)-j}^2 \cdot g_k^{k-j-1} \cdot g_j + C_{n-(k-1)-3(k-1)}^3) + ... =$$

$$= g_k^{n-(k-2)} + C_{n-k}^0 g_k^{n-k} g_1^2 + C_{n-k-1}^0 g_k^{n-k-1} g_1 g_2 + C_{n-k-2}^0 g_k^{n-k-2} g_1 g_3 + ... + C_{n-2k+2}^0 g_k^{n-2k+2} g_1 g_{k-1} +$$

$$+ C_{n-2k+2}^1 g_k^{n-2k+2} g_1 + + C_{n-2k+1}^1 g_k^{n-2k} g_1^3 + C_{n-2k}^1 g_k^{n-2k-1} g_1^2 g_2 + C_{n-2k-1}^1 g_k^{n-2k-2} g_1^2 g_3 + ... +$$

$$+C_{n-3k+3}^{1}g_k^{n-3k+2}g_1^2g_{k-1}+C_{n-3k+3}^{2}g_k^{n-3k+2}g_1^2+C_{n-3k+2}^{2}g_k^{n-3k}g_1^4+C_{n-3k+1}^{2}g_k^{n-3k+1}g_1^3g_2+$$
$$+C_{n-3k}^{2}g_k^{n-3k-2}g_1^3g_3+\ldots+C_{n-4k+4}^{2}g_k^{n-4k+2}g_1^3g_{k-1}+C_{n-4k+4}^{3}g_k^{n-4k+2}g_1^3+\ldots$$

Порівнюючи цей вираз з попереднім видно, що наше припущення є правильним, оскільки, враховуючи припущення, (4) виконується для n. Це і вимагалося довести.

Покажемо, що елементи послідовності U_k можуть бути також обчислені тільки на основі елементів V_k^+ - послідовності.

Для будь-яких цілих додатних n та k, таких що $n \geq k$ отримано таку аналітичну залежність:
$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k} \,. \qquad \textbf{(6)}$$

Проведемо аналіз цієї залежності індукцією по n.

Покажемо, що (6) виконується для n, які дорівнюють $k, k+1, k+2, \ldots, 2k-1$.

$$u_{k,k} = g_k v_{k-1,k} + g_1 g_1 v_{k-2,k} + g_1 g_2 v_{k-3,k} + \ldots + g_1 g_{k-1} v_{0,k} = g_k^2 + g_1^2 \,.$$

$$u_{k+1,k} = g_k v_{k,k} + g_1 g_1 v_{k-1,k} + g_1 g_2 v_{k-2,k} + g_1 g_3 v_{k-3,k} + \ldots + g_1 g_{k-1} v_{1,k} = g_k v_{k,k} + g_1^2 v_{k-1,k} + g_1 g_2 v_{k-2,k}$$

З (3) $v_{k,k} = g_k v_{k-1,k} + g_1 v_{0,k} = g_k v_{k-1,k}$. Враховуючи це, а також значення початкових елементів, отримаємо $u_{k+1,k} = g_k^3 + g_1^2 g_k + g_1 g_2$.

Роблячи таким же чином, знайдемо $u_{k+2,k}$.

$$u_{k+2,k} = g_k v_{k+1,k} + g_1 g_1 v_{k,k} + g_1 g_2 v_{k-1,k} + g_1 g_3 v_{k-2,k} + g_1 g_4 v_{k-3,k} + \ldots + g_1 g_{k-1} v_{2,k} =$$
$$= g_k v_{k+1,k} + g_1 g_1 v_{k,k} + g_1 g_2 v_{k-1,k} + g_1 g_3 v_{k-2,k} = g_k (g_k v_{k,k} + g_1 v_{1,k}) + g_1 g_1 v_{k,k} + g_1 g_2 g_k + g_1 g_3 =$$
$$= v_{k,k}(g_k^2 + g_1 g_1) + g_1 g_2 g_k + g_1 g_3 = (g_k v_{k-1,k} + g_1 v_{0,k})(g_k^2 + g_1 g_1) + g_1 g_2 g_k + g_1 g_3 =$$
$$= g_k^2 (g_k^2 + g_1 g_1) + g_1 g_2 g_k + g_1 g_3 = g_k^4 + g_1 g_1 g_k^2 + g_1 g_2 g_k + g_1 g_3 \ldots$$

$$u_{2k-1,k} = g_k v_{2k-2,k} + g_1 g_1 v_{2k-3,k} + g_1 g_2 v_{2k-4,k} + g_1 g_3 v_{2k-5,k} + \ldots + g_1 g_{k-2} v_{k,k} + g_1 g_{k-1} v_{k-1,k} =$$
$$= g_k (g_k v_{2k-3,k} + g_1 v_{k-2,k}) + g_1 g_1 v_{2k-3,k} + g_1 g_2 v_{2k-4,k} + g_1 g_3 v_{2k-5,k} + \ldots + g_1 g_{k-2} v_{k,k} + g_1 g_{k-1} v_{k-1,k} =$$
$$= (g_k^2 + g_1 g_1) v_{2k-3,k} + g_1 g_2 v_{2k-4,k} + g_1 g_3 v_{2k-5,k} + \ldots + g_1 g_{k-2} v_{k,k} + g_1 g_{k-1} v_{k-1,k} + g_1 g_k v_{k-2,k} =$$
$$= (g_k^2 + g_1 g_1)(g_k v_{2k-4,k} + g_1 v_{k-3,k}) + g_1 g_2 v_{2k-4,k} + g_1 g_3 v_{2k-5,k} + \ldots + g_1 g_{k-2} v_{k,k} + g_1 g_{k-1} v_{k-1,k} +$$
$$+ g_1 g_k v_{k-2,k} = (g_k^3 + g_1 g_1 g_k + g_1 g_2) v_{2k-4,k} + g_1 g_3 v_{2k-5,k} + \ldots + g_1 g_{k-2} v_{k,k} + g_1 g_{k-1} v_{k-1,k} +$$
$$+ g_1 g_k v_{k-2,k} = \ldots = g_k^{k+1} + g_1 g_1 g_k^{k-1} + g_1 g_2 g_k^{k-2} + g_1 g_3 g_k^{k-3} + \ldots + g_1 g_{k-2} g_k^2 + g_1 g_{k-1} g_k + g_1 g_k .$$

Нехай залежність (6) виконується для $n-k, n-k+1, \ldots, n-1$. Покажемо, що вона виконується для n.

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} = g_k^2 v_{n-2,k} + g_1 g_k \sum_{i=1}^{k-1} g_i v_{n-i-2,k} + g_1 g_k v_{n-k-1,k} + g_1^2 \sum_{i=1}^{k-1} g_i v_{n-k-i-1,k} =$$
$$= g_k^2 v_{n-2,k} + g_1 g_k g_1 v_{n-3,k} + g_1 g_k g_2 v_{n-4,k} + \ldots + g_1 g_k g_{k-2} v_{n-k,k} + g_1 g_k g_{k-1} v_{n-k-1,k} +$$
$$+ g_1 g_k v_{n-k+1,k} + g_1^2 g_1 v_{n-k-2,k} + g_1^2 g_2 v_{n-k-3,k} + \ldots + g_1^2 g_{k-2} v_{n-2k+1,k} + g_1^2 g_{k-1} v_{n-2k,k} =$$
$$= g_k (g_k v_{n-2,k} + g_1 v_{n-k-1,k}) + g_1 g_1 (g_k v_{n-3,k} + g_1 v_{n-k-2,k}) + g_1 g_2 (g_k v_{n-4,k} + g_1 v_{n-k-3,k}) + \ldots +$$
$$+ g_1 g_{k-2} (g_k v_{n-k,k} + g_1 v_{n-2k+1,k}) + g_1 g_{k-1} (g_k v_{n-k-1,k} + g_1 v_{n-2k,k}) =$$
$$= g_k v_{n-1,k} + g_1 g_1 v_{n-2,k} + g_1 g_2 v_{n-3,k} + \ldots + g_1 g_{k-2} v_{n-k+1,k} + g_1 g_{k-1} v_{n-k,k} = g_k v_{n-1,k} + g_1 \sum_{i=1}^{k-1} g_i v_{n-i-1,k} .$$

Це і вимагалося довести.

Висновки. Розглянуто рекурентну $\tilde{U_k}$-послідовність, при обчисленні елементів яких використовуються рекурентні залежності з коефіцієнтами, що пов'язані з початковими елементами послідовностей і забезпечується мінімальна складність обчислення елементу.

Отримано аналітичну залежність (4) для безпосереднього обчислення елементів U_k-послідовності, яка показує, що елементи послідовності є поліномом початкових елементів. Отримана залежність надає можливість для оцінювання стійкості криптографічних методів, що можуть бути побудовані на основі U_k-послідовності.

Також отримано залежність (6), яка дозволяє обчислювати елементи U_k–послідовності тільки на основі елементів V_k^+-послідовності, що створює передумови для можливості прискорення обчислень елементу U_k-послідовності.

Представлені рекурентні послідовності, а також сукупність отриманих аналітичних залежностей можуть стати основою математичного апарату для побудови криптографічних методів з відкритим ключем.

Література:

1. Маркушевич А.И. Возвратные последовательности / Маркушевич А.И. – М.: Наука, 1975. – 48 с.
2. Воробьев Н.Н. Числа Фибоначчи / Н.Н. Воробьев. – М.: Наука, 1992. – 192 с.
3. Horadam A.F. A generalized Fibonacci Sequence // Amer. Math. Monthly. – 1961., Vol.68. – P. 455-459.
4. Биркгоф Г. Современная прикладная алгебра: пер. с англ. / Г. Биркгоф, Т. Барти. – М.: Мир, 1976. – 400 с.
5. Кнут Д. Искусство программирования для ЭВМ. Т 2. Получисленные алгоритмы. / Д. Кнут. – М.: Вильямс, 2004. – 832 с.

УДК 004.056.53

Букелкул Салих, асп. *(Гос. университет информационно-коммуникационных технологий)*

ОЦЕНКА СТАЦИОНАРНОЙ СРЕДНЕЙ ОЧЕРЕДИ В СИСТЕМЕ С ОТНОСИТЕЛЬНЫМИ ПРИОРИТЕТАМИ

Букелкул Саліх. Оцінка стаціонарної середньої черги в системі з відносними пріоритетами. Розглянуто приклади знаходженню оцінок стаціонарного середнього часу очікування початку обслуговування вимоги в системі M|GJ|1|∞ з дисциплінами обслуговування без переривання обслуговування.

Ключові слова: СИСТЕМА ОБСЛУГОВУВАННЯ, ВІДНОСНИЙ ПРІОРИТЕТ, СИСТЕМА M|GJ|1|∞

Букелкул Салих. Оценка стационарной средней очереди в системе с относительными приоритетами. Рассмотрены примеры нахождения оценок стационарного среднего времени ожидания начала обслуживания требования в системе M|GJ|1|∞ с дисциплинами обслуживания без прерывания обслуживания.

Ключевые слова: СИСТЕМА ОБСЛУЖИВАНИЯ, ОТНОСИТЕЛЬНЫЙ ПРИОРИТЕТ, M|GJ|1|∞

Boukelkul Salikh. The estimation of stationary average turn in the system with relative priorities. Examples are considered to find estimates of the average time stationary waiting time requirements in the system M|GJ|1|∞ with the disciplines of service without interrupting service.

Keywords: SERVICE SYSTEM, RELATIVE PRIORITIES, SYSTEM M|GJ|1|∞

Система с относительными приоритетами. Рассмотрим систему $M|GJ|1|\infty$ с относительными приоритетами. Предположим, что мы можем выбрать порядок обслуживания требований различных приоритетов, считая, что прерывание обслуживания не допускается. Известно, что в случае конечного числа оптимального (в смысле минимальности) стационарного среднего числа требований в системе (или, что , в силу теоремы Литтла, то же самое – среднего времени ожидания начала обслуживания) порядок обслуживания заключается в преимущественном обслуживании требований из приоритетной группы с наименьшей средней длинной требований. Этот факт вытекает из так называемого