2. Семенко А.І. Особливості проектування телекомунікаційних систем з широкосмуговим шумоподібним сигналом / А.І. Семенко // Вісник Державного університету інформаційно-комуніуаційних технологій. – 2007. – Спецвипуск. – С.108-114.

3. Варакин Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М.: Радио и связь, 1985. – 384 с.

4. Быков В.В. Цифровое моделирование в статистической радиотехнике / В.В. Быков. – М.: Сов. Радио, 1971. – 328 с.

5. Комашинский В.И. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования / В.И. Комашинский, А.В. Максимов. – М.: Горячая линия – Телеком, 2007. – 176 с.

6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом "Вильямс", 2004. – 1104 с.

7. Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем: учеб. пособие для вузов / В.И. Тихонов, В.Н. Харисов. – М.: Радио и связь, 1991. – 608 с.

УДК 511.216

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

ОТРИМАННЯ АНАЛІТИЧНИХ ЗАЛЕЖНОСТЕЙ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ ЕЛЕМЕНТІВ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ РОЗРОБКИ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Яремчук Ю.Є. Отримання аналітичних залежностей прискореного обчислення елементів рекурентних послідовностей для розробки асиметричних криптографічних протоколів. В роботі розглянуто рекурентну U_k-послідовність, для якої встановлено аналітичні залежності прискореного обчислення елементів цієї послідовності через елементи V_k-послідовності. Розглянуті послідовності, а також сукупність отриманих аналітичних залежностей можуть стати основою для розробки асиметричних криптографічних протоколів.

Ключові слова: КРИПТОГРАФІЯ, МАТЕМАТИЧНИЙ АПАРАТ, РЕКУРЕНТНА ПОСЛІДОВНІСТЬ, U_k-ПОСЛІДОВНІСТЬ, V_k-ПОСЛІДОВНІСТЬ

Яремчук Ю.Е. Получение аналитических зависимостей ускоренного вычисления элементов рекуррентных последовательностей для разработки асимметричных криптографических протоколов. В работе рассмотрено рекуррентную U_k-последовательность, для которой установлены аналитические зависимости ускоренного вычисления элементов этой последовательности через элементы V_k-последовательности. Рассмотренные последовательности, а также совокупность полученных аналитических зависимостей, могут стать основой для разработки асимметричных криптографических протоколов.

Ключевые слова: КРИПТОГРАФИЯ, МАТЕМАТИЧЕСКИЙ АППАРАТ, РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, U_k-ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k-ПОСЛЕДОВАТЕЛЬНОСТЬ

Iaremchuk Iu.Ie. Receipt of analytical dependences speed-up calculation of elements of recurrent sequences for development of asymmetric cryptographic protocols. The recurrent is in-process considered U_k-sequence for which analytical dependences of speed-up calculation of elements of this sequence are set through elements V_k-sequences. This sequences, and also aggregate of the got analytical dependences, can to be foundation for development of asymmetric cryptographic protocols.

Keywords: CRYPTOGRAPHY, MATHEMATICAL APPARATUS, RECURRENT SEQUENCE, U_k-SEQUENCE, V_k-SEQUENCE

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

($a_1, a_2, \ldots, a_{\tilde{k}}$ – коефіцієнти; $\tilde{k}$ – порядок послідовності). Відомими прикладами вказаної послідовності є послідовності Фібоначчі [2] та Хорадама [3, 4]. В усіх цих послідовностях початковими елементами є довільні числа, не пов'язані з коефіцієнтами.

Певну цікавість представляють послідовності, в яких початкові елементи пов'язані з коефіцієнтами. Прикладом такої послідовності може бути послідовність, що описана в [5, 6]. В [7] показано можливість спрощення обчислень при побудові асиметричних криптографічних протоколів на основі цієї послідовності. Однак, в роботі [8] було вказано на певну слабкість щодо криптографічної стійкості запропонованого підходу.

Однак пошуки та дослідження рекурентних послідовностей, в яких початкові елементи пов'язані з коефіцієнтами, залишаються актуальними і перспективними, оскільки вони створюють передумови для можливості спрощення обчислень криптографічних перетворень. Для забезпечення цієї можливості важливим є отримання для рекурентних послідовностей аналітичних залежностей прискореного обчислення їх елементів.

Далі пропонуються рекурентні послідовності, а також аналітичні залежності прискореного обчислення елементів, сукупність яких може стати основою для розробки асиметричних криптографічних протоколів.

Отримання аналітичних залежностей прискореного обчислення елементів *U*-послідовності. Назвемо *U*-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 $g_1, g_2, g_3, \ldots, g_k$ – 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

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

Окремим випадком $U_{\tilde{k}}$ послідовності є $V_{\tilde{k}}$ послідовність, елементи якої обчислюються за формулою

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

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 $k > 2$.

Отримано аналітичну залежність, яка дозволяє обчислювати елемент $u_{n+m,k}$ виходячи з елементів $u_{n,k}, u_{n-1,k}, \ldots, u_{n-k+1,k}$. Залежність представляється в такому вигляді.

Для будь-яких цілих додатних n, m та k

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k} \,. \qquad \textbf{(3)}$$

Проведемо аналіз цієї залежності індукцією по m.

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

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

Враховуючи значення початкових елементів, отримаємо $u_{n+1,k} = g_k u_{n,k} + g_1 u_{n-k+1,k}$. Знайдемо тепер $u_{n+2,k}$.

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

З (2) $v_{k,k} = g_k v_{k-1,k} + g_1 v_{0,k} = g_k v_{k-1,k}$. Тоді $u_{n+2,k} = g_k v_{k-1,k} u_{n,k} + g_1 v_{k-1,k} u_{n-k+1,k} + g_1 v_{k-2,k} u_{n-k+2,k} =$
$= v_{k-1,k}(g_k u_{n,k} + g_1 u_{n-k+1,k}) + g_1 u_{n-k+2,k} = g_k u_{n+1,k} + g_1 u_{n-k+2,k}$.

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

$$u_{n+3,k} = v_{k+1,k} u_{n,k} + g_1 v_{k,k} u_{n-k+1,k} + g_1 v_{k-1,k} u_{n-k+2,k} + g_1 v_{k-2,k} u_{n-k+3,k} + g_1 v_{k-3,k} u_{n-k+4,k} + \ldots + g_1 v_{2,k} u_{n-1,k} =$$
$$= (g_k v_{k,k} + g_1 v_{1,k}) u_{n,k} + g_1 v_{k,k} u_{n-k+1,k} + g_1 v_{k-1,k} u_{n-k+2,k} + g_1 u_{n-k+3,k} =$$
$$= v_{k,k}(g_k u_{n,k} + g_1 u_{n-k+1,k}) + g_1 v_{k-1,k} u_{n-k+2,k} + g_1 u_{n-k+3,k} = v_{k,k} u_{n+1,k} + g_1 v_{k-1,k} u_{n-k+2,k} + g_1 u_{n-k+3,k} =$$
$$= (g_k v_{k-1,k} + g_1 v_{0,k}) u_{n+1,k} + g_1 v_{k-1,k} u_{n-k+2,k} + g_1 u_{n-k+3,k} =$$
$$= v_{k-1,k}(g_k u_{n+1,k} + g_1 u_{n-k+2,k}) + g_1 u_{n-k+3,k} = g_k u_{n+2,k} + g_1 u_{n-k+3,k}\,;$$ і т.д..

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

Нехай залежність (3) виконується для $m-k$, $m-k+1$, ... , $m-1$. Покажемо, що вона виконується для m.

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

Залежність (3) показує, що елементи U_k-послідовності обчислюються через елементи двох послідовностей U_k і V_k^+.

Виходячи з формули (1) вираз для обчислення елементів для спадних n, починаючи з деякого $n = l$, має такий вигляд:

$$u_{n,k} = \frac{u_{n+k,k} - g_k u_{n+k-1,k}}{g_1}\,. \qquad \textbf{(4)}$$

Запишемо аналогічну формулу для елементів $V_k^{\tilde{+}}$ послідовності:

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}\,. \qquad \textbf{(5)}$$

Для будь-яких цілих додатних n та m таких, що $1 < m < n$ отримано таку аналітичну залежність

$$u_{n-m,2} = (-1)^m \cdot g_1^{-(m-1)} \cdot (v_{m-2,2} \cdot u_{n,2} - v_{m-1,2} \cdot u_{n-1,2})\,. \qquad \textbf{(6)}$$

Проведемо аналіз цієї залежності індукцією по m. Покажемо, що (6) виконується для $m=2$ і $m=3$.

$$u_{n-2,2}=g_1^{-1}\cdot(v_{0,2}u_{n,2}-v_{1,2}u_{n-1,2})=g_1^{-1}\cdot(u_{n,2}-g_2u_{n-1,2}).$$

$$u_{n-3,2}=-g_1^{-2}\cdot(v_{1,2}u_{n,2}-v_{2,2}u_{n-1,2})=-g_1^{-2}\cdot(g_2u_{n,2}-(g_2^2+g_1)\cdot u_{n-1,2})=$$

$$=g_1^{-2}\cdot(-g_2u_{n,2}+g_2^2u_{n-1,2}+g_1u_{n-1,2})=-\frac{g_2}{g_1}\cdot\frac{u_{n,2}-g_2u_{n-1,2}}{g_1}+\frac{u_{n-1,2}}{g_1}=\frac{u_{n-1,2}-g_2u_{n-2,2}}{g_1}.$$

Нехай залежність (6) виконується для $m+1$, $m+2$. Покажемо, що вона виконується для m. Згідно формули (1)

$$u_{n-m,2}=g_2u_{n-m-1,2}+g_1u_{n-m-2,2}=g_2u_{n-(m+1),2}+g_1u_{n-(m+2),2}=$$

$$=(-1)^{m+1}g_1^{-m}g_2(v_{m-1,2}u_{n,2}-v_{m,2}u_{n-1,2})+(-1)^{m+2}g_1^{-m}(v_{m,2}u_{n,2}-v_{m+1,2}u_{n-1,2})=$$

$$=(-1)^{m}g_1^{-m}(-g_2v_{m-1,2}u_{n,2}+g_2v_{m,2}u_{n-1,2}+v_{m,2}u_{n,2}-v_{m+1,2}u_{n-1,2})=$$

$$=(-1)^{m}g_1^{m-1}\cdot(\frac{v_{m,2}-g_2v_{m-1,2}}{g_1}u_{n,2}-\frac{v_{m+1,2}-g_2v_{m,2}}{g_1}u_{n-1,2}).$$

Враховуючи формулу (4), отримаємо $u_{n-m,2}=(-1)^m g_1^{-(m-1)}\cdot(v_{m-2,2}u_{n,2}-v_{m-1,2}u_{n-1,2})$. Це і вимагалося довести.

Введемо в розгляд $V_k^{\sim}$ послідовність, елементи якої обчислюються за формулою (5) для n – від'ємних при початкових значеннях $v_{-1,k}=0$, $v_{-2,k}=g_1^{-1}$ для $k=2$; $v_{-1,k}=0$, $v_{-2,k}=g_1^{-1}$, $v_{-3,k}=v_{-4,k}=\ldots=v_{-k,k}=0$ для $k>2$.

Тоді послідовність чисел, яка складається з V_k^+–послідовності та V_k^-–послідовності назвемо V_k – послідовністю.

Залежність (6) встановлює зв'язок між елементами послідовності U_k і V_k^+, але це є окремий випадок при $k=2$. Для будь-яких k послідовності U_k притаманна така властивість.

Для будь-яких цілих додатних n і m, таких що $1\le m<n$ та будь-якого цілого додатного k отримано таку залежність

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

Проведемо аналіз цієї залежності індукцією по m.

Покажемо, що (7) виконується для m, які дорівнюють 1, 2 , 3, . . . , k.

$$u_{n-1,k}=v_{k-3,k}u_{n,k}+g_1v_{k-4,k}u_{n-k+1,k}+\ldots+g_1v_{-1,k}u_{n-2,k}+g_1v_{-2,k}u_{n-1,k}.$$

Враховуючи значення початкових елементів, отримаємо $u_{n-1,k}=g_1g_1^{-1}u_{n-1,k}=u_{n-1,k}$.

Знайдемо тепер $u_{n-2,k}$.

$$u_{n-2,k}=v_{k-4,k}u_{n,k}+g_1v_{k-5,k}u_{n-k+1,k}+\ldots+g_1v_{-1,k}u_{n-3,k}+g_1v_{-2,k}u_{n-2,k}+g_1v_{-3,k}u_{n-1,k}=g_1v_{-2,k}u_{n-2,k}=u_{n-2,k}.$$

$$u_{n-k,k}=v_{-2,k}u_{n,k}+g_1v_{-3,k}u_{n-k+1,k}+\ldots+g_1v_{-k,k}u_{n-2,k}+g_1v_{-k-1,k}u_{n-1,k}=$$

$$=v_{-2,k}u_{n,k}+g_1v_{-k-1,k}u_{n-1,k}=g_1^{-1}u_{n,k}+g_1(-g_kg_1^{-2})u_{n-1,k}=\frac{u_{n,k}-g_ku_{n-1,k}}{g_1}=u_{n-k,k}.$$

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

$$u_{n-m,k}=g_ku_{n-m-1,k}+g_1u_{n-m-k,k}=$$

$$=g_kv_{-m-1+(k-2),k}u_{n,k}+g_1g_k\sum_{i=1}^{k-1}v_{-m-1+(k-2)-i,k}u_{n-k+i,k}+g_1v_{-m-k+(k-2),k}u_{n,k}+g_1^2\sum_{i=1}^{k-1}v_{-m-k+(k-2)-i,k}u_{n-k+i,k}=$$

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

Це і вимагалося довести.

Висновки. Розглянуто рекурентні $U_k^{\sim}$ послідовності, при обчисленні елементів яких використовуються рекурентні залежності з коефіцієнтами, що пов'язані з початковими елементами послідовностей.

Отримано аналітичні залежності (3), (6), (7) відповідно прискореного обчислювання елементів U_k-послідовності для зростаючих n через елементи $U_k^{\sim}$ та $V_k^{\mp}$ послідовностей; прискореного обчислення елементів послідовності для спадних n, для випадку, коли $k = 2$, з використанням елементів V_k^{+}-послідовності; прискореного обчислення елементу $u_{n,k}$ для спадних n для будь-якого k з використанням елементів V_k^{-}-послідовності.

Отримані аналітичні залежності дозволяють обчислити певний елемент послідовності виходячи з деяких елементів, не використовуючи послідовності рекурентних обчислень, що значно прискорює процес обчислень і створює можливість для розробки асиметричних криптографічних протоколів.

Література

1. Маркушевич А.И. Возвратные последовательности / А.И. Маркушевич. – 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. Vol.68, 1961. Pp. 455459.

4. Биркгоф Г. Современная прикладная алгебра: пер. с англ. / Г. Биркгоф, Т. Барти. – М.: Мир. 1976. – 400 с.

5. H. Lehmer. An extended theory of Lucas' functions.: Annals of Math, 1930. Pp. 4199448.

6. Smith P. and Lennon M. LUC: A new public key system // Proceedings of the IFIP TC11 Ninth International Conference on Information Security. North-Holland, 1993. Pp.103-117.

7. Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology Asiacrypt '94. Springer-Verlag, 1995. – Pp. 357-364.

8. Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology Crypto '95. Springer-Verlag, 1995. – Pp. 386-396.