two identically zero roots and two simple roots which are identically double. Due to the method of essential singular functions the new regularizing variable is obtained and the extension of the vector equation is kept. Asymptotic forms of solutions for the homogeneous problem are constructed with the help of Airy functions and their derivatives. Asymptotic forms of solutions for the nonhomogeneous problem are constructed using Scorer functions. The article discusses the variation of the non-stable turning point or the variation when the turning point is on the left of origin.

Keywords: linear system, small parameter, turning point, space of the nonresonance solutions, Airy-Langer model operator, Orr–Sommerfeld type equation.

Одержано редакцією 17.08.2016 Прийнято до друку 21.09.2016

УДК 62-50:519.7 PACS 05

В.В. Кириченко, Є.В. Лесіна

ОСОБЛИВОСТІ ДИСКРЕТНИХ АЛГОРИТМІВ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ОБЕРНЕНИХ ДИНАМІЧНИХ СИСТЕМ

Комп'ютерна реалізація алгоритмів перетворення інформації на основі хаотичної динаміки приводить до необхідності дискретизації систем. Робота присвячена вивченню особливостей обернених дискретних систем керування як перетворювачів інформації, зокрема, такої їхньої властивості, як динамічна деградація. Вона полягає в можливому різкому зменшенні дискретної множини станів складної динамічної системи при введенні інформаційного повідомлення. В значній мірі це явище залежить від початкових значень траєкторій та параметрів системи. Наведено приклад динамічної системи, траєкторії якої мають складну внутрішню динаміку, але при введенні в неї інформаційного повідомлення потрапляють на нульовий інваріантний многовид. Тим самим, замість шифрування вхідної інформаційної послідовності, вихід системи для будь-яких значень ключових параметрів, починаючи з деякого моменту, в точності передає значення інформаційного входу з одиничною затримкою.

Ключові слова: обернені динамічні системи, динамічна деградація, кільце цілих чисел, генератори псевдовипадкових послідовностей, шифрування, функція керування.

Вступ

У зв'язку з розвитком супутникових, мобільних, комп’ютерних комунікаційних систем зростає значення проблеми конфіденційності передачі інформації і більш широкої проблеми захисту інформації на ринку комунікаційних послуг. У наш час виникає нагальна потреба у захисті комерційної інформації в комп'ютерних мережах, забезпечення безпеки електронних платежів та інтернет-телефонії і таке ін. Типовою вимогою стає необхідність масового застосування алгоритмів кодування та їх низька собівартість на одиницю «інформаційної» продукції. В останній час, з появою роботи

[1], інтенсивно вивчаються можливості використання в телекомунікаційних технологіях динамічних систем, які мають хаотичну поведінку ([2,3,4]).

Встановлено, що при масовому розв'язанні «побутових» проблем захисту інформації можуть успішно застосовуватися потокові алгоритми шифрування, у тому числі і такі, що базуються на динамічних системах з хаотичною поведінкою траєкторій.

Актуальною проблемою стає вивчення можливостей використання хаотичних систем у комунікаційних технологіях та розробка і апробування ряду конкретних алгоритмів і схем хаотичного кодування, що забезпечують керований ступінь конфіденційності. Ці схеми повинні забезпечити: а) високу ефективність захисту мультимедійної інформації; б) великі швидкості кодування; в) високу стійкість стосовно шуму. При розв'язанні проблем захисту інформації може бути успішно застосована методика, заснована на детермінованому хаосі, який породжується нелінійними динамічними системами. При цьому слід визначити наступні властивості динамічних систем, які забезпечують можливість їхнього використання [5].

Базовим для таких систем є властивість оберненості, тобто можливість відновлювати зовнішній вхід (інформаційне повідомлення) нелінійної динамічної системи за її виходом (сигналом, що направляється в комунікаційні мережі). Явище оберненості широко використовується в багатьох задачах теорії керування складними системами.

Доведення факту хаотичності траєкторій для тієї або іншої динамічної системи є складною математичною проблемою.

Комп'ютерна реалізація алгоритмів перетворення інформації на основі динамічних систем, які мають наведені вище властивості, приводить до необхідності дискретизації систем. Тому стає актуальним питання дослідження інформаційних характеристик дискретних комп'ютерних реалізацій алгоритмів кодування (статистичні властивості, розпізнавання постійних послідовностей символів, розмір алфавіту, вплив перешкод), а також алгоритмів кодування, які використовують властивості динамічних систем з хаотичною поведінкою. Ця проблема вивчається, наприклад, в роботах [6,7].

1. Особливості дискретних систем керування

Схеми визначення невідомого входу за інформацією про вихід системи, розглянуті для неперервних систем, можуть бути використані і для дискретних систем, динаміка яких визначена рівняннями

$$\begin{aligned} x(k+1) &= f(x(k),u(k)),\\ y(k) &= h(x(k)). \end{aligned} \tag{1}$$

У системі (1) вихід не залежить явно від вхідної інформаційної послідовності $u(k)$. Визначимо аналогічно неперервному випадку поняття відносного порядку входу. Значення функції $h\big(f(x,u)\big)$ може не залежати від значень u, тому аналогічно і $y(k+1)=h\big(f(x(k),u(k)\big)$ може не містити $u(k)$. Визначимо, на яку кількість кроків відбувається затримка між інформацією на вході і виході системи (1). Ця величина саме вказує на відносний порядок входу в системі (1).

Покладемо $f^i(x,u)=f\circ f\cdots\circ f(x,u), i\ge 1$, де $\circ$ позначає суперпозицію функцій. Будемо говорити, що система (1) має відносний порядок $r>0$, якщо для всіх x,u

$$\frac{\partial(h\circ f^i(x,u))}{\partial u}\equiv 0,\ i=1,\dots,r-1,$$

$$\frac{\partial(h\circ f^r(x,u))}{\partial u}\neq 0.$$

Таким чином, відносний порядок r для дискретної системи вказує на номер елемента вихідної послідовності, на який явно впливає перший елемент вхідної послідовності $u(0)$. Перетворення координат

$$\begin{pmatrix}\xi\\ \eta\end{pmatrix}=\begin{pmatrix}f^r(x)\\ \Phi(x)\end{pmatrix},\quad \det\frac{\partial(f^r(x),\Phi(x))}{\partial x}\neq 0,$$

приводить систему (1) до нормальної форми

$$\begin{cases}\xi_i(k+1)=\xi_{i+1}(k),\\ \xi_r(k+1)=F(\xi(k),\eta(k),u(k)),\\ \eta\,(k+1)=G(\xi(k),\eta(k),u(k)),\quad i=1,\ldots,r,\end{cases}\tag{2}$$

де, як і в неперервному випадку, ξ,η визначають як внутрішню, так і зовнішню динаміку відповідно. Розв'язуючи відносно $u(k)$ рівняння

$$\xi_r(k+1)=F(\xi(k),\eta(k),u(k)),$$

знаходимо

$$u(k)=g\big(\xi_r(k+1),\xi(k),\eta(k)\big).\tag{3}$$

Після підстановки (3) у (2) одержуємо обернену дискретну динамічну систему

$$\eta(k+1)=G(\xi_r(k+1),\xi(k),\eta(k)).\tag{4}$$

Отже, для відновлення повідомлення, заданого послідовністю $u(k)$, додатково до значень сигналу $\xi_1(k),\ldots,\xi_r(k),\xi_r(k+1)$ необхідно мати інформацію про $n-r$ початкові умови $\eta(0)$ динамічної системи (4). Таким чином, для динамічних систем, представлених у дискретній формі, можуть бути використані алгоритми, розроблені для неперервних систем. Модифікація відбувається за рахунок заміни значень похідних від сигналу на відповідне значення виходу дискретної системи, отримане з запізнюванням, рівним порядку похідної.

2. Стійкість алгоритмів розшифрування до помилок сигналу

Розглянемо дискретні реалізації описаних динамічних систем і поставимо задачу визначення їхніх характеристик, як потокових динамічних шифраторів інформаційної послідовності $\{u(k),k=1,\ldots N\}$. Перехід до операцій над полем цілих чисел дозволяє усунути цілий ряд труднощів, що виникають при використанні дискретних динамічних систем. Основна проблема пов'язана з тією обставиною, що використання багатомірних систем приводить до надлишкових обчислень. При використанні машинної арифметики з комою, що плаває, надмірність обчислювальних операцій над інформаційним масивом приводить до

а) помітного росту часу обробки даних;

б) швидкого росту помилки обчислень.

Набагато більш високу швидкість розрахунків, причому без помилок, забезпечує обчислювальний пристрій з фіксованою комою. Крім того, такого роду обчислювальні пристрої легко можуть бути реалізовані у виді цифрових шифраторів-дешифраторів, розташованих у місцях входів і виходів потоку даних інформаційної системи в загальну комунікаційну мережу.

Розглянемо одномірну дискретну систему, праві частини якої не залежать від зовнішнього впливу (відсутня модуляція системи інформаційним сигналом $u(k)$):

$$x(k+1)=F\big(x(k)\big)$$

Нехай використовувана обчислювальним пристроєм машинна точність складає L біт. Тоді будь-яка величина A, представлена в двійковому коді, має вид $A\ mod\ 2L$, тобто

значення A містяться у множині $\{0,1,2,...,2L-1\}$. У зв'язку з тим, що міра цілочисельних точок у просторі R^n дорівнює нулю, динамічна система, записана в скінченому полі з $2L$ елементами, не може адекватно описувати динаміку хаотичної системи, що її породжує.

Зокрема, наслідком детермінованості і того факту, що простір станів $x(k)$ визначено $2L$ значеннями $\{0,1,2,...,2L-1\}$, є наступний висновок:

Усяка траєкторія системи з початковою умовою x(0) в полі цілих чисел за модулем 2L буде періодичною з періодом TX(0), як правило, меншим за 2L. Таким чином, один із критеріїв хаотичності динамічної системи – неперервний спектр розв'язків – не виконаний. Цілочисельна траєкторія має дискретний спектр, кратний TX(0).

Отже, для динамічної системи в полі цілих чисел за модулем $2L$ метод хаотичного маскування, при якому сигнал, що передається, несе інформацію у формі $y(k) = x(k) + u(k)$, не змінює частотних властивостей повідомлення $u(k)$.

3. Результати

У випадку n-мірної системи (1) кількість різних станів фазового вектору $x(k)$ зростає до $2L \cdot n$. Комп'ютерне моделювання процесу шифрування-розшифрування за зазначеною схемою показує, що при деяких початкових умовах та параметрах системи (які значно відрізняються від початкового стану передавача) великі інформаційні масиви можуть відновлюватися за допомогою приведеної оберненої системи практично без перекручувань. Вказана обставина є небажаним явищем, бо зменшує криптографічні якості схеми шифрування.

Ефект виродження власної динаміки системи при введенні в праву частину неавтономного обурення, виражений у вигляді падіння розмірності простору станів, назвемо динамічною деградацією.

Для вивчення цього ефекту наведемо наступний приклад. Розглянемо передавач (шифратор), побудований на базі рівнянь Ейлера, які описують рух твердого тіла і сконструюємо відповідну обернену систему [6]. Для виявлення ефекту деградації підберемо спеціальні параметри передавача: коефіцієнти в правих частинах дорівнюють одиниці, а виходом буде друга координата. Таким чином, маємо нелінійну систему вхід-вихід, на вхід якої подається повідомлення $u(k)$:

$$\begin{aligned} x_1(k+1) &= x_2(k) \cdot x_3(k) \bmod 2L, \\ x_2(k+1) &= x_1(k) \cdot x_3(k) + u(k) \bmod 2L, \\ x_3(k+1) &= x_1(k) \cdot x_2(k) \bmod 2L, \\ y(k) &= x_2(k). \end{aligned} \tag{5}$$

Сигнал $y(k)$ направляється в комунікаційну мережу. Ключем для розшифрування є невідомі початкові умови системи $x_1(0), x_2(0), x_3(0)$. Приймач (дешифратор) – це обернена система, за допомогою якої при відомому ключі проводиться відновлення значень $u(k)$ за формулами:

$$\begin{aligned} x_1(k+1) &= x_2(k) \cdot x_3(k) \bmod 2L, \\ x_2(k+1) &= y(k+1), \\ x_3(k+1) &= x_1(k) \cdot x_2(k) \bmod 2L, \\ u(k) &= y(k+1) - x_1(k) \cdot x_3(k) \bmod 2L. \end{aligned}$$

Напишемо перші ітерації значення сигналу $k = 0, 1, 2, 3, 4, 5, 6$:

$$y(0) = x_2(0),$$

$$y(1) = x_1(0)x_3(0) + u(0),$$

$$y(2) = x_1(1)x_3(1) + u(1) = x_2^2(0)x_1(0)x_3(0) + u(1),$$

$$y(3) = x_1(2)x_3(2) + u(2) = \left[x_1(0)x_3(0) + u(0)\right]^2 x_1(1)x_3(1) + u(2) =$$
$$= \left[x_1(0)x_3(0) + u(0)\right]^2 x_2^2(0)x_1(0)x_3(0) + u(2),$$

$$y(4) = x_1(3)x_3(3) + u(3) = \left[x_2^2(0)x_1(0)x_3(0) + u(1)\right]^2 x_1(2)x_3(2) + u(3) =$$
$$= \left[x_2^2(0)x_1(0)x_3(0) + u(1)\right]^2 \cdot \left[x_1(0)x_3(0) + u(0)\right]^2 \cdot x_2^2(0) \cdot x_1(0)x_3(0) + u(3),$$

$$y(5) = x_1(4)x_3(4) + u(4) = \left[\left[x_1(0)x_3(0) + u(0)\right]^2 x_2^2(0)x_1(0)x_3(0) + u(2)\right]^2 x_1(3)x_3(3) + u(4) =$$
$$= \left[\left[x_1(0)x_3(0) + u(0)\right]^2 x_2^2(0)x_1(0)x_3(0) + u(2)\right]^2 \cdot \left[x_2^2(0)x_1(0)x_3(0) + u(1)\right]^2 \times$$
$$\times \left[x_1(0)x_3(0) + u(0)\right]^2 \cdot x_2^2(0) \cdot x_1(0)x_3(0) + u(4),$$

$$y(6) = x_1(5)x_3(5) + u(5) =$$

$$= \left[\left[x_2^2(0)x_1(0)x_3(0) + u(1)\right]^2 \cdot \left[x_1(0)x_3(0) + u(0)\right]^2 \cdot x_2^2(0) \cdot x_1(0)x_3(0) + u(3)\right]^2 x_1(4)x_3(4) + u(5) =$$
$$= \left[\left[x_2^2(0)x_1(0)x_3(0) + u(1)\right]^2 \cdot \left[x_1(0)x_3(0) + u(0)\right]^2 \cdot x_2^2(0) \cdot x_1(0)x_3(0) + u(3)\right]^2 \times$$
$$\times \left[\left[x_1(0)x_3(0) + u(0)\right]^2 x_2^2(0)x_1(0)x_3(0) + u(2)\right]^2 \cdot \left[x_2^2(0)x_1(0)x_3(0) + u(1)\right]^2 \times$$
$$\times \left[x_1(0)x_3(0) + u(0)\right]^2 \cdot x_2^2(0) \cdot x_1(0)x_3(0) + u(5).$$

З отриманих формул випливає наступне рекурентне співвідношення для визначення $u(k)$:

$$\begin{cases} y(0) = x_2(0), \\ y(1) = u(0) + x_1(0)x_3(0), \\ y(k) = u(k-1) + x_1(0)x_3(0)\prod\limits_{i=0}^{k-2} y^2(i), \quad k \geq 2. \end{cases}$$

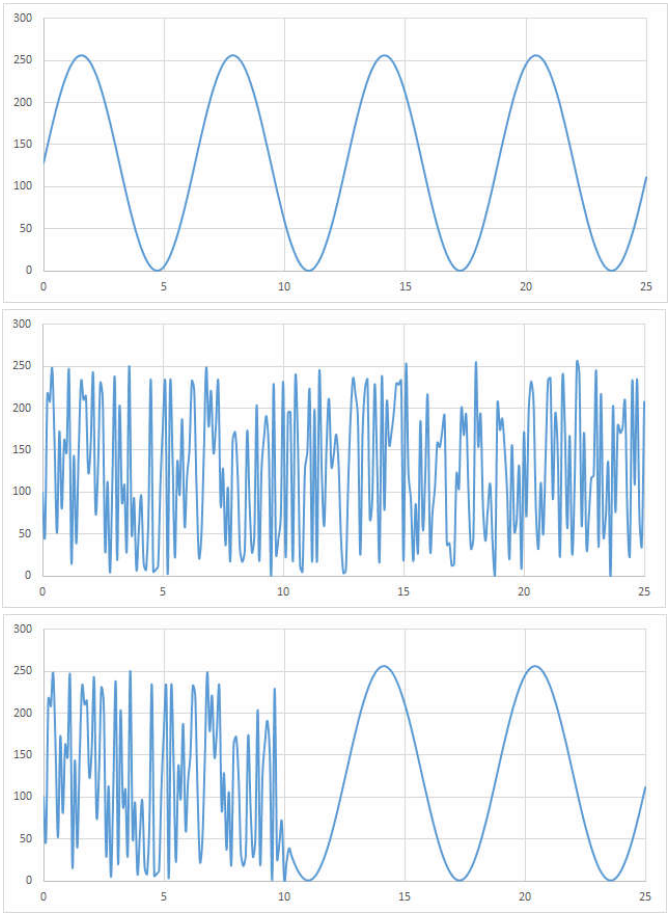
Звідси знаходимо

$$u(k-1) = \begin{cases} y(k) - x_1(0)x_3(0), \quad k = 1, \\ y(k) - x_1(0)x_3(0)\prod\limits_{i=0}^{k-2} y^2(i), \quad k \geq 2. \end{cases}$$

Для цієї задачі має місце наступне твердження:

Твердження. Нехай для деякого цілого N значення сигналу системи (5) $y(N) = x_1(N)x_3(N) + u(N) = 0 \pmod{2L}$. Тоді для будь-якого $i > N+1$ маємо: $y(i) = u(i-1)$.

Для демонстрації цього ефекту в якості вхідного сигналу візьмемо функцію $u(x) = 128\sin(x) + 128$ (рис. 1, а), та закодуємо його за допомогою системи (5) при $L = 128$. Результат кодування показано на рис. 1, *б*. Якщо на деякому кроці підібрати значення функції $u(x)$ таким чином, щоб виконувалась умова твердження, то буде мати місце ефект деградації (рис. 1, *в*).



а б в

Рис.1. *а* – кодування періодичного сигналу, б – без ефекту деградації, в – з ефектом деградації.

Таким чином, замість шифрування інформаційної послідовності $u(k)$, вихід розглянутої динамічної системи для будь-яких значень ключових параметрів, починаючи з деякого моменту, передає значення входу з одиничною затримкою.

Висновки

Один з перспективних напрямків розвитку сучасних телекомунікаційних технологій пов'язаний з використанням нелінійних динамічних систем, що володіють хаотичним поводженням. Базовою для таких систем є властивість оберненості, тобто можливість відновлювати вхідний вплив (інформаційне повідомлення) на нелінійну динамічну систему за її виходом (сигналом), що направляється в комунікаційні мережі.

У роботі обговорюються питання побудови різних типів зворотних систем, у залежності від наявної інформації про початковий стан і параметри передавача.

Комп'ютерна реалізація алгоритмів перетворення інформації на основі хаотичної динаміки приводить до необхідності дискретизації систем. Вивчення особливостей обернених дискретних систем керування як перетворювачів інформації дозволило експериментально виявити ефект динамічної деградації при деяких значеннях параметрів динамічних систем. Вона полягає в можливому різкому зменшенні дискретної множини станів складної динамічної системи при введенні інформаційного повідомлення. Наведено приклад динамічної системи, траєкторії якої мають складну внутрішню динаміку, але при введенні в неї інформаційного повідомлення потрапляють на нульовий інваріантний многовид. Таким чином, замість шифрування вхідної інформаційної послідовності, вихід системи для будь-яких значень ключових

параметрів, починаючи з деякого моменту, в точності передає значення інформаційного входу з одиничною затримкою.

Список використаної літератури:

1. Sobhy M. J. Secure computer communication using chaotic algorithms / M. J. Sobhy, A. Shehata. //Int. J. of Bifurcation and Chaos. – vol. 10, no. 12, 2000.– P. 2831–2839.

2. Щербак В.Ф. Обратные системы управления в коммуникационных технологиях / В.Ф. Щербак, В.В. Кириченко. // Тр. Ин-та прикл. математики и механики НАН Украины. – 2003. – 8. – С. 244-252.

3. Кириченко В.В. Особенности информационной системы управления БПЛА / В.В. Кириченко, Е.В. Лесина // Наукові праці Донецького національного технічного університету. Серія: «Інформатика, кібернетика та обчислювальна техніка». – №1 (22), 2016. – С.111-116.

4. Ковалев А.М. Обобщенная обратимость динамических систем в задачах шифрования /А.М. Ковалев, В.А. Козловский, В.Ф. Щербак //Прикладная дискретная математика.– №1, 2009. – С. 20–21.

5. Рябко Б.Я. Криптографические методы защиты информации / Б.Я. Рябко, А.Н. Фионов – М: Горячая линия-Телеком. 2005, – 232 с.

6. Ковалев А.М. Обратимые динамические системы с переменной размерностью фазового пространства в задачах криптографического преобразования информации/ А.М. Ковалев, В.А. Козловский, В.Ф. Щербак // Прикладная дискретная математика.– №2(2),2008. – С. 39–44.

7. Дмитриев А.С. Динамический хаос как парадигма современных систем связи / А.С. Дмитриев, А.И. Панас, С.О. Старков // Зарубежная радиоэлектроника. – №10, 1997.– С.4-25.

References

15. Sobhy M. J. And Shehata A. (2000). Secure computer communication using chaotic algorithms. *Int. J. of Bifurcation and Chaos*, vol. 10, no. 12, 2000, 2831–2839.

16. ScsherbackV.F., KyrychenkoV.V. (2003). Come back control systems in communication technology. *Proceedings of the Institute of Applied Mathematics and Mechanics of NAS of Ukraine*, 8, 244-252.

17. KyrychenkoV.V., LesinaYe.V. (2016). Features of information UAV control system. *Scientific papers of Donetsk National Technical University. Series: "Informatics, Cybernetics and Computer Science"*,№1 (22), 111-116.

18. Kovalev A.M., Kozlovsky V.A., Scsherback V.F. (2009). Generalized reversibility of dynamical systems in the encryption tasks. *Applied Discrete Mathematics*, №1, 20–21.

19. Ryabko B.Ya., Fionov A.N. (2005). Cryptographic methods of information protection. *M: HotlineTelecom*, 232.

20. Kovalev A.M., Kozlovsky V.A., Scsherback V.F. (2008). Inverse dynamical systems with variable dimension of phase space in problems of cryptographic information transformation. *Applied Discrete Mathematics*, № 2(2), 39–44.

21. Dmitriev A.S., Panas A.I., Starkov S.O. (1997) . Dynamic chaos as a paradigm of modern communication systems. *International electronics*, № 10, 4-25.

Summary. ***V.V. Kyrychenko, Ye.V. Lesina. Features of discrete algorithms data transform using inverse dynamic systems.*** *In view of development of satellite, mobile, computer and communication systems, it is evident the importance of issues of confidentiality information transfer and broader issues of information security in the market of communication services. The actual problem studies the possibilities of using chaotic systems*

and communication technologies in the development and testing of a number of specific algorithms and coding schemes chaotic, providing a controlled degree of confidentiality. These schemes should provide: high efficiency protection of multimedia data, high speed encoding; high resistance concerning noise. In solving the problems of information security can be successfully applied technique based on deterministic chaos, which is generated by non-linear dynamic systems.

The base for such systems is inverse property, i.e. the possibility to restore external input (Announcement) nonlinear dynamical system on its output (the signal is sent to the communication network). Inverse phenomenon is widely used in many problems of control theory of complex systems.

Systems that have chaotic dynamics are an important feature - they are synchronized. This fact is widely used in many algorithms for encryption and decryption. The receiving device in these algorithms instead of the original system uses its observer.

Here are the main ways of encoding information using dynamic chaos. Input signal in transmitter through the unknown input. Parametric modulation. Use masking.

We consider the properties of nonlinear dynamic systems with chaotic behavior as transducers information and the features of discrete control systems and decryption algorithms resistance error signal.

Computer algorithms realization conversion information based on chaotic dynamics leads to the need for sampling systems. This work concerns investigation of inverse discrete control systems as data processors, including their properties such as dynamic degradation. It is a sharp decrease in the discrete set of states of complex dynamic systems introduced in the Announcement. To a large extent this phenomenon depends on the initial values of the trajectories and system parameters. In this paper we consider the example of a dynamic system, trajectories which have a complex integral dynamic, but it introduced an information notice fall to zero invariant variety. Thus, instead of encrypting the input information sequence output system for any values of key parameters, starting from some point exactly conveys important information from the input unit delay.

Keywords: inverse dynamic systems, dynamic degradation, ring of integers, generators pseudorandom sequences, encryption, control function.

Одержано редакцією 25.08.2016 Прийнято до друку 27.09.2016