УДК 681.3.06

О.О. Кузнецов[1], В.Ю. Ковтун[2], Ю.М. Рябуха[1]

[1]*Харківський університет Повітряних Сил імені І. Кожедуба, Харків*
[2]*Національний авіаційний університет, Київ*

ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ ІЗ ВИКОРИСТАННЯМ МОДУЛЯРНИХ ПЕРЕТВОРЕНЬ

Розглядаються методи формування псевдовипадкових послідовностей із використанням модулярних перетворень. Досліджуються правила формування псевдовипадкових чисел та періодичні властивості відповідних послідовностей. Розробляється удосконалений метод, який за рахунок додаткового введення рекурентних перетворень дозволяє формувати послідовності максимального періоду та позбутися наявності слабких ключів.

Ключові слова: *псевдовипадкова послідовність, модулярне перетворення, ключ, рекурентність.*

Постановка, проблеми у загальному вигляді та аналіз літератури

Проведені дослідження показали, що модулярні криптоперетворення являють собою потужний математичний апарат, який широко застосовується для побудови доказово стійких криптографічних засобів захисту інформації, у тому числі і доказово стійких генераторів псевдовипадкових послідовностей (ПВП) [1-6]. Однак, в ході досліджень з'ясовано, що відомі доказово стійкі генератори, що засновані на використанні модулярних перетворень володіють певними недоліками щодо періодичних властивостей та наявності слабких ключів [7]. Вони не можуть бути використовувані у системах управління критичного застосування, в тому числі і у системах криптографічного захисту від несанкціонованого доступу.

Метою статті **є** розробка удосконаленого методу формування ПВП, який, за рахунок додаткового введення рекурентних перетворень дозволяє формувати послідовності максимального періоду та позбутися наявності слабких ключів, що підвищує ефективність та розширює можливості щодо практичного використання.

1. Використання модулярних перетворень для формування псевдовипадкових послідовностей

Модулярні перетворення широко застосовуються в сучасних методах формування псевдовипадкових чисел [3-6]: в генераторах Рівеста-Шаміра-Аделмана (RSA), Мікалі-Шнора (MS) та Блюм-Блюм-Шаба (BBS). Однак, як з'ясовано у [7], вказані генератори мають слабкі ключі, використання яких призводить до катастрофічно низьких значень періоду формованих послідовностей. Встановлено, що для кожного дослідженого генератора існують такі значення ключових даних, використання яких призводить до виродженої роботи генератора, коли формована послідовність має детермінований вигляд із дуже малим значенням періоду (одиниці-десятки символів).

Розглянемо правила формування псевдовипадкових чисел відповідними генераторами та обґрунтуємо шляхи щодо їх удосконалення.

Спосіб формування ПВП із використанням перетворень RSA [4], ґрунтується на тому, що ключова послідовність подається у вигляді вектору x_0, який ініціює початкове значення аргументу функції $f(x) = x^e \bmod n$ модульного зведення у ступінь. У якості модуля n обирається добуток великих простих чисел p і q, у якості ступеня e обирається число, взаємно просте з числом $(p-1)\cdot(q-1)$. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у ступінь а вихідні елементи ПВП формуються шляхом зчитування значення функції модульного зведення за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

$$b_0 \quad b_1 \quad b_2 \quad \dots \quad b_i \quad \dots \quad b_{m-1}, \; i = \overline{0,(m-1)},$$

де b_i – молодший біт числа x_i,

$$x_{i+1} = f(x_i) = x_i^e \bmod n.$$

Задача вираховування функції $f(x)^{-1}$, яка є зворотною до функції модульного зведення у ступінь $f(x) = x^e \bmod n$, тобто вирахування деякого значення x_i за відомим значенням x_{i+1} є важкорозв'язуваною теоретико-складною задачею дискретного логарифмування, щодо вирішення якої на сьогоднішній день невідомо ефективних алгоритмів вираховування дискретних логарифмів великих чисел [3].

Аналіз правила формування ПВП із використанням перетворень RSA показує, що формовані послідовності не є максимальними. Це випливає з того, що послідовне виконання модульного зведення

© О.О. Кузнецов, В.Ю. Ковтун, Ю.М. Рябуха

$x_i^e \bmod n$ не завжди дає максимальний цикл формованих значень $x_{i+1} = x_i^e \bmod n$. Це експериментально доведено у [7], період формованих ПВП значно менший за максимальний.

Спосіб формування ПВП із використанням перетворень MS є деякою модифікацією розглянутого способу із RSA перетвореннями [3, 5]. У якості модуля n обирається добуток великих простих чисел p і q, у якості ступеня e обирається число, взаємно просте з числом $(p-1)\cdot(q-1)$, причому число e відповідає нерівності $80 \cdot e \le N$, де N - збільшена на одиницю бітова довжина числа n, тобто $N = \lfloor \log_2 n \rfloor + 1$. Шуканою послідовністю біт довжини $m \cdot k$ буде послідовність

$$z_0 \parallel z_1 \parallel z_2 \parallel \dots z_i \parallel \dots z_{m-1} \parallel,\ i = \overline{0,(m-1)},$$

де: z_i – k молодших бітів числа y_i; $z_i \parallel z_j \parallel$ – конкатенація бітів із z_i та із z_j; x_{i+1} – r старших бітів числа y_i, причому

$$y_i = f(x_i) = x_i^e \bmod n,\ k = \left\lfloor N \cdot \left(1 - \frac{2}{e}\right) \right\rfloor,\ r = N - k.$$

Генератор ПВП із використанням перетворень MS має значно підвищену швидкість формування. Це обумовлено тим, що з кожного обрахованого значення x_{i+1} у якості елементів ПВП зчитується не один біт (як у способі із RSA перетвореннями) а k бітів, тобто швидкість формування ПВП збільшено у k разів. Однак періодичні властивості ПВП не покращено. Період послідовності обчислених значень x_{i+1} не змінюється (в порівнянні із RSA перетвореннями).

Спосіб формування ПВП із використанням перетворень BBS ґрунтується на тому [6], що ключова послідовність x_0 ініціює початкове значення аргументу функції $f(x) = x^2 \bmod n$ модульного зведення у квадрат. У якості модуля n обирається добуток великих простих чисел p і q, які тотожні трьом за модулем чотири, тобто:

$$p \equiv 3 \bmod 4,\ q \equiv 3 \bmod 4,\ n = p \cdot q,$$

де n - ціле число Блюма [3].

Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у квадрат а шуканою послідовністю біт довжини m буде послідовність

$$b_0\ \ b_1\ \ b_2\ \ \dots\ \ b_i\ \ \dots\ \ b_{m-1},\ i = \overline{0,(m-1)},$$

де b_i - молодший біт числа x_i,

$$x_{i+1} = f(x_i) = x_i^2 \bmod n.$$

Задача вираховування примітивних квадратних коренів за модулем числа n обчислювально еквівалентна задачі розкладення цього числа на множники, тобто важкорозв'язуваної теоретико-складної задачі факторизації.

Періодичні властивості генератору BBS є також незадовільними, періоди формованих послідовностей менші за максимальні на 2-5 порядків, при збільшенні довжини максимального періоду ця різниця збільшується [7].

Для покращення періодичних властивостей розглянутих генераторів ПВП доцільно застосувати рекурентні перетворення над формованими значеннями x_{i+1} (позначимо їх як сеансові ключі). При відповідному правилі побудови рекурентних перетворень послідовність формованих значень x_{i+1} та і відповідна ПВП будуть максимальними.

2. Удосконалений метод формування ПВП максимального періоду

Метод відрізняється від відомих введенням рекурентних перетворень над сеансовими ключовими послідовностями, які в сукупності з використовуваними модулярними перетвореннями дозволяють забезпечити побудову доказово стійких генераторів ПВП максимального періоду. Пропонований метод дозволяє формувати ПВП максимального періоду із використанням перетворень RSA, MS та BBS [8, 9].

Формування ПВП максимального періоду із використанням перетворень RSA полягає в тому, що ключова послідовність подається у вигляді вектору x_0, який ініціює початкове значення аргументу функції $f(x) = x^e \bmod n$ модульного зведення у ступінь та початкове значення y_0 рекурентного перетворення $L(y)$, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками [8]. У якості модуля n обирається добуток великих простих чисел p і q, у якості ступеня e обирається число, взаємно просте з $(p-1)\cdot(q-1)$. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у ступінь та за допомогою рекурентного перетворення, що реалізується, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками. Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного зведення за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

$$b_0\ \ b_1\ \ b_2\ \ \dots\ \ b_i\ \ \dots\ \ b_{m-1},\ i = \overline{0,(m-1)},$$

де b_i - молодший біт числа x_i,

$$x_{i+1} = f(x_i + L(y_i)) = (x_i + L(y_i))^e \bmod n.$$

Задача вираховування функції $f(x)^{-1}$, яка є зворотною до функції модульного зведення у ступінь

$f(x) = x^e \bmod n$, тобто вирахування деякого значення $x_i + L(y_i)$ за відомим значенням x_{i+1} є важкорозв'язуваною теоретико-складною задачею дискретного логарифмування, щодо вирішення якої на сьогоднішній день невідомо ефективних алгоритмів вираховування дискретних логарифмів великих чисел. Тому цей спосіб формування ПВП є криптографічно стійким. Додатково введене рекурентне перетворення $L(y)$ дозволяє формувати послідовності псевдовипадкових чисел максимального періоду. Запропонований метод може бути реалізовано у вигляді пристрою, структурна схема якого зображена на рис. 1.

Рис. 1. Структурна схема пристрою формування ПВП максимального періоду із використанням перетворень RSA

Пристрій функціонує наступним чином [8]. В блок вводу ключових даних вводиться послідовність Key, яка виступає у якості секретного ключа. Вона передається у блок формування початкових станів, який призначений для ініціювання рекурентної функції модульного зведення у ступінь та рекурентного перетворення, що формує послідовність максимального періоду (наприклад, лінійного рекурентного регістру максимального періоду).

Сформовані початкові стани x_0 та y_0 подаються на входи відповідних пристроїв: значення y_0 подається на блок рекурентного перетворення (наприклад, шляхом заповнення лінійного рекурентного регістру); значення x_0 подається на блок додавання, на другий вхід якого подається значення, зняте з виходу блока рекурентного перетворення $L(y_i)$ (на першій ітерації з виходу блока рекурентного перетворення може бути зчитане значення $L(y_0) = y_0$ як стан лінійного рекурентного регістру). Блок додавання формує суму $L(y_i) + x_i$, значення якої подається на блок модульного зведення у ступінь. У блоку модульного зведення у ступінь розраховується значення $x_{i+1} = f(x_i + L(y_i)) = (x_i + L(y_i))^e \bmod n$, яке подається на вхід блоку формування вихідної послідовності та на вхід блоку додавання. В блоку формування вихідної послідовності зі значення x_{i+1} зчитується найменш значущій біт даних (біт парності), який подається на вихід пристрою як елемент псевдовипадкової послідовності. Наступна ітерація роботи пристрою починається з подання на блок додавання з блоку модульного зведення у ступінь значення x_{i+1}. Одночасно, блок рекурентного перетворення формує наступне значення $L(y_{i+1})$ (наприклад, шляхом виконання процедури зсуву у лінійному регістрі) та видачі отриманого значення, яке також подається на блок додавання. Блок додавання формує суму $L(y_{i+1}) + x_{i+1}$, яка подається на блок модульного зведення у ступінь і операція повторюється. Блок узгодження призначений для погодження роботи окремих блоків пристрою та управління процесом формування псевдовипадкової послідовності. Пристрій зупиняє свою роботу за командою блоку узгодження (зупинку можна здійснити на кожному кроці).

Формалізовано роботу пристрою при застосуванні лінійних рекурентних регістрів (позначимо їх через LRR) можна подати у такий спосіб.

Секретний ключ: Key;

Початковий стан: x_0 = Key, y_0 = Key;

Циклова функція:

$$f(x + LRR(y)) = ((x + LRR(y))^e) \bmod (n),$$

$$LRR(y=\{u_1, u_2, \ldots, u_m\}): u_i = -\Sigma_j a_j u_{i-j} + u_i,$$

де $n = pq$, $\gcd(e, \varphi(p,q)) = 1$, $\varphi(p,q) = (p-1)(q-1)$, $\{u_1, u_2, \ldots, u_m\}$ – стан LRR, $\{a_1, a_2, \ldots, a_m\}$ – коефіцієнти, які задають функцію зворотного зв'язку LRR;

Формована псевдовипадкова послідовність:

$$(b_0, b_1, \ldots, b_i, \ldots)$$

де b_i – найменш значущій біт (біт парності) числа x_i,

$$x_i = f(x_{i-1} + LRR(y_{i-1})) = ((x_{i-1} + LRR(y_{i-1}))^e) \bmod (n),$$

$$y_i = LRR(y_{i-1}).$$

Таким чином, за рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, вдається формувати ПВП максимального періоду, що підвищує ефективність та розширює можливості практичного використання.

Використання перетворень MS для формування ПВП максимального періоду формалізовано опишемо у такий спосіб.

Секретний ключ: Key;

Початковий стан: x_0 = Key, y_0 = Key;

Циклова функція:

$$f(x + LRR(y)) = ((x + LRR(y))^e) \bmod (n),$$

$$LRR(y=\{u_1, u_2, \ldots, u_m\}): u_i = -\Sigma_j a_j u_{i-j} + u_i,$$

де n = pq, gcd(e,φ(p,q)) = 1, φ(p,q) = (p-1)(q-1), 80e ≤ ≤ N, N = [$\log_2 n$] + 1, {u_1, u_2, …, u_m} – стан LRR, {a_1, a_2, …, a_m} – коефіцієнти, які задають функцію зворотного зв'язку LRR;

Формована псевдовипадкова послідовність:

$$(z_0 \| z_1 \| \dots \| z_i \| \dots)$$

де z_i – k найменш значущих бітів числа w_i,

$$w_i = f(x_{i-1} + LRR(y_{i-1})) = ((x_{i-1} + LRR(y_{i-1}))^e) \bmod(n),$$

$$y_i = LRR(y_{i-1}),$$

$z_i \| z_{i+1}$ – конкатенація бітового подання чисел z_i і z_{i+1}, x_i – r старших бітів числа w_i,

$$r = N - k,\ k = [N(1-2/e)].$$

Для випадку використання перетворень BBS замість блоку модульного зведення у ступінь використовується відповідний блок модульного зведення у квадрат з накладеними обмеженнями на відповідні прості числа (числа Блюма): $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$. Формалізовано роботу пристрою при застосуванні лінійних рекурентних регістрів можна подати у такий спосіб [9].

Секретний ключ: Key;

Початковий стан: x_0 = Key, y_0 = Key;

Циклова функція:

$$f(x + LRR(y)) = ((x + LRR(y))^2) \bmod(n),$$

$$LRR(y=\{u_1, u_2, \dots, u_m\}): u_i = -\Sigma_j a_j u_{i-j} + u_i,$$

де n = pq (ціле число Блюма), p = (3)mod(n), q = (3)mod(n), {u_1, u_2, …, u_m} – стан LRR, {a_1, a_2, …, a_m} – коефіцієнти, які задають функцію зворотного зв'язку LRR;

Формована псевдовипадкова послідовність:

$$(b_0, b_1, \dots, b_i, \dots)$$

де b_i – найменш значущій біт (біт парності) числа x_i,

$$x_i = f(x_{i-1} + LRR(y_{i-1})) = ((x_{i-1} + LRR(y_{i-1}))^2) \bmod(n),$$

$$y_i = LRR(y_{i-1}).$$

Таким чином, за рахунок додаткового введення рекурентних перетворень, вдається формувати ПВП максимального періоду, що підвищує ефективність та розширює можливості практичного використання розглянутих генераторів.

3. Дослідження властивостей запропонованих генераторів ПВП

Для підтвердження достовірності та обгрунтованості отриманих результатів шляхом експериментальної перевірки періодичних властивостей формованих послідовностей, для підтвердження відсутності слабких ключів, що призводять до виродженої роботи та формування детермінованих послідовностей з критично низькими значеннями довжин періоду було розроблено програмну реалізацію запропонованих генераторів. Експериментальні дослідження полягали у вивченні періодичних властивостей відповідних генераторів шляхом повного перебору всіх ключових послідовностей, оцінці відповідних довжин періоду L формованих ПВП та порівнянні із максимальною довжиною періоду L_{max}.

При проведені експериментальних досліджень було обрано вихідні дані, відповідно до проведених у [7] досліджень. Отримані результати зведені на рис. 2, 3.

На рис. 2 зображено розподіл довжин періодів формованих послідовностей для запропонованого методу формування ПВП (чорний колір) із використанням перетворень RSA, а саме розподіл кількості ключів по довжинам відповідних періодів формованих послідовностей для кожного із досліджуваних випадків. На рисунку наведено також відомості про наявні довжини періодів у відомому методі-прототипі (сірий колір).

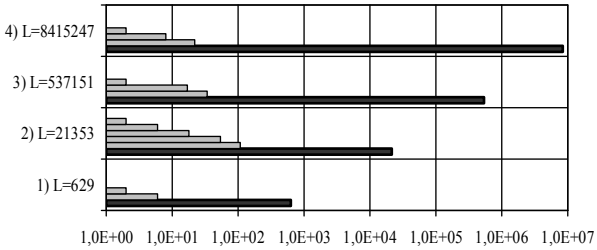

Рис. 2. Результати дослідження періодичних властивостей генераторів ПВП із використанням перетворень RSA

Як видно із наведених даних запропоновані генератори ПВП володіють покращеними періодичними властивостями. Так для першого експерименту ПВП із довжиною періоду L = 629 формуються при введені всіх ключів (всі цілі числа від 2 до 628), тобто всі формовані псевдовипадкові числа x_{i+1} згруповані у одну послідовність максимального періоду із довжиною 629. В той же час для методу-прототипу існують ключі, введення яких призводить до формування ПВП з періодом $L \in [1, 2, 6]$.

Аналогічні результати маємо і для трьох інших експериментів:

- введення всіх ключів (всі цілі числа від 2 до 21352) призводить до формування ПВП із довжиною періоду L = 21353 (експеримент 2). Для методу прототипу $L \in [1, 2, 6, 18, 54, 108]$;
- введення всіх ключів (всі цілі числа від 2 до 537150) призводить до формування ПВП із довжиною періоду L = 537151 (експеримент 3). Для методу прототипу $L \in [1, 2, 17, 34]$;
- введення всіх ключів (всі цілі числа від 2 до 8415246) призводить до формування ПВП із довжиною періоду L = 8415247 (експеримент 4). Для методу прототипу $L \in [1, 2, 22]$.

Аналогічні результати було отримано і при дослідженні періодичних властивостей генераторів ПВП із використанням перетворень BBS, для яких розподіл кількості ключів по довжинам відповідних періодів формованих послідовностей наведено на рис. 3.

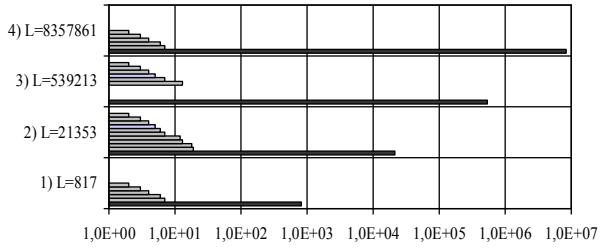

Рис. 3. Результати дослідження періодичних властивостей генераторів ПВП із використанням перетворень BBS

Як видно з наведених даних всі формовані псевдовипадкові числа згруповані у одну послідовність максимального періоду із довжиною n, тобто кожен із використовуваних ключів дозволяє формувати послідовність максимального періоду. Іншим чином поводить себе метод-прототип. Відповідний генератор ПВП не задовольняє вимогам щодо періодичних властивостей формованих ПВП, існують слабкі ключі з катастрофічно низькими значеннями довжини періодів.

Таким чином, проведені дослідження довели, що запропоновані генератори псевдовипадкових чисел володіють покращеними періодичними властивостями. Для кожного із введених ключів період формованих послідовностей є максимальним, тобто можна стверджувати, що запропоновані генератори позбавлені наявності слабких ключів.

Висновки

Проведені дослідження довели, що застосування модулярних перетворень дозволяє будувати ефективні доказово стійкі генератори ПВП. Теоретично обґрунтоване введення рекурентних перетворень, що реалізуються наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, дозволяє покращити періодичні властивості формованих послідовностей та позбавитися наявності слабких ключів.

За своїми властивостями пропоновані генератори можуть бути використовувані у системах управління критичного застосування, в тому числі і у підсистемах системах криптографічного захисту від несанкціонованого доступу.

Перспективним напрямком подальших досліджень є обґрунтування пропозицій щодо вдосконалення механізмів криптографічного захисту інформації, які використовують генератори ПВП.

Список літератури

1. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 - Version 0.15 (beta), Springer-Verlag. – P. 829.

2. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.

4. Shamir A. On the generation of cryptographically strong pseudorandom sequences / A. Shamir // ACM Transactions on Computer Systems. – 1983. – Vol. 1. – P. 38-44.

5. Blum, M. How to generate cryptographically strong sequences of pseudo-random bits / M. Blum, S. Micali // SIAM Journal on Computing. – 1984. – Vol. 13. – P. 850-864.

6. Blum L. A simple unpredictable pseudorandom number generator / L. Blum, M. Blum, M. Shub // SIAM Journal on Computing. – 1986. – Vol. 15. –P. 364-383.

7. Рябуха Ю.М. Метод формування псевдовипадкових послідовностей максимального періоду із використанням модулярних перетворень / Ю.М. Рябуха // Системи озброєння і військова техніка. – 2009. – Вип. 4 (20). – С. 166-169.

8. Кузнецов О.О. Євсеєв С.П., Рябуха Ю.Н., Корольов Р.В., Пудов В.А. Спосіб формування послідовностей псевдовипадкових чисел / Пат. UA 38402 U, МКІ (2006) G09C 1/00. – № и 200810861; Заявл. 03.09.2008; Опубл. 12.01.2009, Бюл. №1, 2009р. – 4 с.

9. Кузнецов О.О. Євсеєв С.П., Рябуха Ю.Н., Корольов Р.В., Пудов В.А. Спосіб формування послідовностей псевдовипадкових чисел. Пат. UA 39674 U, МКІ (2009) G09C 1/00. – № и 200810863; Заявл. 03.09.2008; Опубл. 10.03.2009, Бюл. №5, 2009р. – 4 с.

Надійшла до редколегії 13.05.2010

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ФОРМИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОГО ПЕРИОДА С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНЫХ ПРЕОБРАЗОВАНИЙ

А.А. Кузнецов, В.Ю. Ковтун, Ю.Н. Рябуха

Рассматриваются методы формирования псевдослучайных последовательностей с использованием модулярных превращений. Исследуются правила формирования псевдослучайных чисел и периодические свойства соответствующих последовательностей. Разрабатывается усовершенствованный метод, который за счет дополнительного введения рекуррентных превращений позволяет формировать последовательности максимального периода и лишиться наличия слабых ключей.

Ключевые слова: *псевдослучайная последовательность, модулярное преобразование, ключ, рекуррентность.*

FORMING OF ПСЕВДОСЛУЧАЙНЫХ SEQUENCES OF MAXIMAL PERIOD WITH THE USE OF MODULYARNYKH OF TRANSFORMATIONS

A.A. Kuznecov, V.Yu. Kovtun, Yu.N. Ryabukha

The methods of forming of pseudo-random sequences are examined with the use of modular transformations. The rules of forming of pseudo-random numbers and periodic properties of the proper sequences are explored. The improved method which due to additional introduction of recurrent transformations allows to form the sequences of maximal period and deprived presences of the weak keys is developed.

Keywords: *pseudo-random sequence, modular transformation, key, recurrentness.*