УДК 681.324.067

Т.О. Гріненко, Ю.І. Горбенко

Харківський національний університет радіоелектроніки

ВЛАСТИВОСТІ ДЕТЕРМІНОВАНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ЩО ГЕНЕРУЮТЬСЯ НА ОСНОВІ БАГАТОМОДУЛЬНИХ ПЕРЕТВОРЕНЬ В ПОЛЯХ ГАЛУА

Визначаються умови існування псевдовипадкових послідовностей з рівно ймовірним розподілом символів m-го алфавіту в класі багатомодульних перетворень та даються оцінки нижніх границь необоротності.

Ключові слова: *псевдовипадкова послідовність, багатомодульне перетворення, поле Галуа, необоротність.*

Вступ

В деяких криптографічних додатках виникає необхідність в використанні псевдовипадкових послідовностей (ПВП) з певною основою алфавіту m та певними властивостями необоротності, нерозрізнюванстi, а також гарантованим періодом повторення. До таких перетворень можна віднести багатомодульні перетворення [1]. В [1] запропоновано метод генерування ПВП на основі багатомодульного перетворення в полі Галуа $GF(p)$, який дозволяє генерувати ПВП з довільним алфавітом та заданим (необхідним) періодом повторення.

В теоретичному змісті властивості багатомодульного перетворення елементів поля Галуа GF(P) за простими модулями $p, p_1, p_2, \ldots, p_{k-1}$, на перший погляд, не викликали сумнівів [1]. Але проведені експериментальні дослідження показали необхідність уточнення вимог до взаємних властивостей простого числа p – першого модуля перетворення та інших модулів – $p_1, p_2, \ldots, p_{k-1}, m$. В першу чергу, це відноситься до модулів $p_1, p_2, \ldots, p_{k-1}, m$ та їх співвідношеннями із модулем p. При багатомодульному перетворенні, що пропонується в [1], особливу властивість має можливе розповсюдження символів, в першу чергу, нуля. Нерозглянутими також залишилися питання застосування в генераторах такого типу ключових даних, тобто розробки криптографічного генератора, а також оцінки рівнів гарантій такого генератора ПВП в частині необоротності та нерозрізнюваності.

Основною метою цієї статі є уточнення методу генерування ПВП з певним алфавітом символів m, на основі багатомодульних перетворень з використанням елементів поля Галуа $GF(p)$, а також дослідження властивостей необоротності та нерозрізнюваності.

1. Умови існування ДГВП на основі багатомодульного перетворення

В статі [1] доведено, що на основі багатомодульних перетворень можна побудувати послідовності *q*-ічних ПВЧ як завгодно великого періоду, при цьому, теоретично обгрунтовано, що на всій довжині періоду поява будь-якого числа з інтервалу $[0, q-1]$ практично рівноймовірна. Обґрунтованість такого підходу пов'язана з тим, що у більшості застосувань достатньо трьох модульного перетворення, а при чотирьох та більше перетвореннях властивості зберігаються.

При розгляді будемо вважати, що елементи поля Галуа генеруються згідно такого правила

$$b_i = \left(\left(\theta_j\right)^{K_0+i} (\mathrm{mod}(p), (p_1), (m))\right), \qquad (1)$$

де $K_0 + i$ є плинний ключ генератора, K_0 – початковий ключ, а i – ключ сеансу.

Для умови (1) має місце теорема 1, що запропонована та доведена нами в процесі досліджень.

Теорема 1. Детермінований генератор випадкових чисел (ДГВЧ), що функціонує згідно багатомодульного перетворення на основі (1) забезпечує генерування детермінованих випадкових (псевдовипадкових) символів (цілих чисел) з періодом повторення $p-1$, рівноймовірно і з певною основою алфавіту m, за умови, що:

$$p_1 | p-1, \text{ а } m | p_1 - 1. \qquad (2)$$

Доведемо теорему для 3-ьох модульного перетворення.

Відносно періоду повторення. Так як θ_j первісний елемент, а p – просте число, то

$$a_i = \left(\left(\theta_j\right)^i (\mathrm{mod}(p))\right) \qquad (3)$$

має період $p-1$, а кожен елемент поля з'являється один раз. Це витікає безпосередньо із властивостей простого поля Галуа $GF(p)$ [2].

Для визначення умов рівноймовірності формування символів згідно (1) обчислимо усі елементи поля (3) для $i = \overline{0, p-1}$ та подамо їх у вигляді цілих натуральних чисел від $\theta_j^0 = 1$ до $p-1$. Це буде один із ізоморфізмів поля Галуа, який визначається однозначно первісним елементом θ_j [2].

Далі упорядкуємо числа ізоморфізму $1 \div p-1$ в міру збільшення, тобто у вигляді

$$1, 2, 3, \ldots, p-1 \qquad (4)$$

та приведемо ряд (4) по модулю p_1. Замітимо, що при цьому в упорядкованому блоці кожне з чисел від 1 і до $p-1$ міститься один раз, тобто як і раніше. В результаті приведення по модулю p_1 отримаємо

$$\begin{gathered} 1, 2, 3, \ldots, p_1-1, 0, 1, 2, 3, \ldots \\ \ldots, p_1-1, 0, 1, 2, 3, \ldots, p_1-1, \ldots, 0, 1, \ldots, V, \end{gathered} \qquad (5)$$

де $0 \le V \le |p_1 - 1|$.

При $V = 0$ значення p_1 буде кратним $p-1$ і тоді безпосередній аналіз ряду (5) підтверджує рівноймовірність появи символів алфавіту p_1. При $V \ne 0$ значення p_1 не буде кратним $p-1$ і в ряді (5) будуть ще і символи $1,2,\ldots,V$. Тобто частота появи цих символів на 1 буде більшою ніж $V+1, V+2, \ldots, p_1-1$. За даних умов ряд (5) можна подати у такому вигляді

$$\begin{gathered} \overbrace{1, 2, 3, \ldots, p_1-1}^{1}; \overbrace{0, 1, 2, 3, \ldots, p_1-1}^{2}; \ldots \\ \ldots; \overbrace{0, 1, 2, 3, \ldots, p_1-1}^{z-1}; \overbrace{0, 1, 2, 3, \ldots, V}^{z}, \end{gathered} \qquad (6)$$

причому $V \le p_1 - 1$.

Всього в ПВП буде $(z-1)p_1 + V$ елементів (символів) послідовності алфавіту p_1. Тому за умови коли $V = 0$, ймовірність R_1 появи символів алфавіту p_1

$$R_1 = \frac{z-1}{p-1} = \frac{p-1}{p_1(p-1)} = \frac{1}{p_1}. \qquad (7)$$

Коли $V \ne 0$, один раз додатково появляються ще і символи $1,2,\ldots,V$, тому ймовірність R_2 появи символів $1,2,\ldots,V$ із множини $1, 2, 3, \ldots, p_1-1$ буде більшою, і по аналогії з (7) буде дорівнювати

$$R_2 = \frac{z}{p-1}. \qquad (8)$$

Таким чином, на періоді $p-1$ послідовності в результаті виконання перетворення ще і по другому модулю, коли p_1 буде кратним $p-1$, символи алфавіту з основою p_1, тобто $1, 2, 3, \ldots, p_1-1, 0$, появляються з однаковою ймовірністю рівноймовірно, інакше з несуттєвим відхиленням, яке визначається (8).

Розглянемо етап перетворення по третьому модулю, який згідно твердження може задовольняти чи не задовольняти вимозі (2), наприклад, бути довільним цілим числом m чи вибраним спеціальним чином. Будемо вважати, що вимога (2) виконується, та доведемо, що у цьому випадку символи ПВП, які генеруються згідно (1), появляються на періоді повторення рівноймовірно.

Відмітимо, що доведення цієї частини твердження також необхідно виконати відносно (1), тобто відносно елементів поля Галуа (3), які перетворені за модулем p_1. Далі, так як розглядається частості появи символів алфавіту m, то для підтвердження умови забезпечення рівноймовірності можна розглядати уже впорядковану послідовність (6). Якщо при цьому m кратне $p_1 - 1$, то приводячи по модулю m послідовність $1,2,3,\ldots,p_1-1,0$, отримаємо

$$\begin{gathered} 1, 2, 3, \ldots, m-1, 0; \; 1, 2, 3, \ldots, m-1, 0; \ldots \\ \ldots; 1, 2, 3, \ldots, m-1, 0. \end{gathered} \qquad (9)$$

Такі ж результати отримаємо і при $m = 2$, тобто для двійкової послідовності

$$1,0; \; 1,0; \ldots; 1,0. \qquad (10)$$

Безпосередньо із (6) витікає, що ймовірність R_1 появи кожного із символів уже m-го алфавіту, за умови виконання (2), дорівнює

$$R_1 = \frac{1}{(p-1)/m} = \frac{m}{p-1}, \qquad (11)$$

причому кожен символ алфавіту на періоді появляється

$$n = \frac{p-1}{m} \qquad (12)$$

разів. Тобто, при приведенні за модулем m отримаємо $(p-1)/m$ блоків розміру m, а кожен із них містить точно один m-й символ. Теорема 1 доведена.

Для підтвердження справедливості теореми розглянемо приклад. Нехай p=4001, p_1=100, m=5, 10 та 20. Безпосереднім моделюванням підтверджено теоретичні оцінки (11) та (12). Так при m=5, на періоді 4000, символи 0,1,2,3,4 появляються n=800 разів, при m=10 символи 0,1,2,3,4,5,6,7,8,9 появляються n=400 разів, при m=20 символи 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19 появляються n=200 разів кожен.

В той же час інтерес має випадок, коли не виконується умова (2), наприклад p_1 є простим числом 101, а m=20. В даному випадку, що підтверджується результатами моделювання, виникає ефект розмноження нулів. Він пов'язаний з тим, що m не кратне p_1. Тому в (6) при приведенні по модулю m додатково появляються нулі. Якщо ж виконується умова (2), то вона є і достатньою умовою рівноймовірності появи символів при трьох модульному перетворенні.

Замітимо, що при доведенні теореми 1 одночасно визначені вимоги і до модуля m. Більш детально вимоги до параметрів p, p_1, m та властивості багатомодульного перетворення в залежності від параметрів наведені в [1].

2. Властивості багатомодульного перетворення в полі Галуа GF(p)

Важливими є задачі вивчення властивостей необоротності ПВП.

Нижче наводяться пропозиції з оцінки криптографічної стійкості генераторів багатомодульних

перетворень, що будуються з використанням полів Галуа. Так як основним визнаним методом забезпечення стійкості є криптографічний, то розглянемо в основному захищеність ключів від їх можливої компрометації.

Для оцінки криптографічної стійкості генератора багатомодульних перетворень будемо розглядати два класи атак – аналітичні атаки та атаки груба сила [3].

Метою реалізації вказаних атак є визначення ключа генератора $(K_0 + i)$ в (1). Відомими будемо вважати l символів b_i вихідної ПВП, загальні параметри

$$p, p_1, \ldots, p_{k-1}, m, \qquad (13)$$

а також значення первісного елемента θ_j. В цьому випадку задачі зводяться до вирішення задач обернення (1) для поля $GF(p)$.

Нині добре вирішені питання здійснення криптографічних атак на дискретний логарифм виду (1), яке по аналогії з асиметричною криптографією будемо називати атакою типу повне розкриття. Необхідно також відмітити, що властивості необоротності по суті пов'язані з розв'язком дискретного логарифмічного рівняння (1) відносно i та $K_0 + i$ (K_0).

Спочатку зробимо аналіз для випадку одномодульного перетворення. Згідно [3] розроблено та застосовуються ряд методів для вирішення дискретного логарифмічного рівняння. В нашому випадку необхідно розв'язувати, на наш погляд, набагато складніші дискретні логарифмічні рівняння виду (1), тобто для багато- або трьохмодульного перетворення.

При аналізі стійкості будемо вважати, що метою атаки є визначення конкретного значення таємного ключа $K_0 + i$ (K_0), що застосовується. В цьому випадку необхідно вирішити дискретне логарифмічне рівняння. В результаті буде відомий ключ $K_0 + i$ (K_0), знання якого дозволить побудувати певний відрізок елементів ПВП. При вирішенні в такій постановці задачі криптоаналізу вважається, що криптоаналітику відомі загальні параметри та послідовність l елементів b_i. У випадку, коли застосовується гешування, задача, на наш погляд, суттєво ускладнюється, так як значення елементів уже невідомі, а відомі тільки геш-значення від цих елементів. Тому, в цьому випадку, спочатку необхідно вирішувати задачу визначення прообразу зі складністю $I_{пр} = 2^n - 1$ [3], а вже потім вирішувати задачу дискретного логарифмування. Цей випадок розглядається нижче.

Для розв'язку задач дискретного логарифмування в простому полі Галуа можуть бути застосовані атаки типу «груба сила» та аналітичні атаки. Перші атаки не будемо розглядати, так як при прийнятих значеннях довжин ключів $K_0 + i$ (K_0) згідно [3] $l_k \geq 256$ бітів, складність атаки буде складати порядку 2^{256} це $\approx 10^{77}$. Навіть деяка оптимізація атак «груба сила» не приводить до практичного зменшення складності дискретного логарифмування.

Тут зробимо попередні оцінки, що задача повного розкриття зводиться до вирішення дискретного логарифму в полі $I_{дл}$ і носить субекспоненційний характер виду [3]

$$I_{дл} = \exp\left(\varepsilon \ln(p)^{\upsilon} \ln\ln(p)^{(1-\upsilon)}\right), \qquad (13)$$

де (ε, υ) параметри методу дискретного логарифмування в полі Галуа.

Так для методу загального решета числового поля параметри методу приймемо $(\varepsilon, \upsilon) = (1.9018, 1/3)$, тому (13) буде мати вигляд

$$I_{дл} = \exp\left(1.9018 \ln(p)^{1/3} \ln\ln(p)^{(1-1/3)}\right). \qquad (14)$$

Ряд атак, що направлені на вирішення дискретного логарифмічного рівняння виду (14) ґрунтуються на використанні методу узагальненого парадоксу про день народження [3]. В [3] показано, що для випадку застосування методу ρ - Полларда складність атаки I_ρ може бути визначена як

$$I_\rho = \sqrt{-2n\ln(1-P_k)} = \sqrt{-2^{l+1}\ln(1-P_k)}. \qquad (15)$$

Підкреслимо, що наведені вище формули можуть бути застосованими тільки для оцінки складності вирішення дискретного логарифмічного рівняння виду (16), тобто для одномодульного перетворення

$$b_i = \left(\left(\theta_j\right)^{K_0+i} (\mathrm{mod}(p))\right). \qquad (16)$$

Зробимо оцінки стійкості для випадку поки що вирішення дискретного логарифмічного рівняння та застосування перетворення типу гешування. В цьому випадку спочатку необхідно знайти прообраз відповідного елемента поля A_i зі складністю $I_{пр}$, а потім вирішити дискретне логарифмічне рівняння зі складністю (14) $I_{дл}$. Враховуючи сказане вище, в тому числі послідовність подій, маємо таку оцінку складності знаходження ключа (але ще раз наголосимо, що це для випадку одномодульного перетворення)

$$I_{\Gamma_1} = I_{дл} I_{пр} = \left(2^n - 1\right) \times \\ \times \exp\left(1.9018 \ln(p)^{1/3} \ln\ln(p)^{(1-1/3)}\right). \qquad (16)$$

Для випадку застосування ρ - Полларда метода замість (16) отримаємо

$$I_{\Gamma_2} = I_{дл} I_\rho = 2^{n/2} \times \\ \times \exp\left(1.9018 \ln(p)^{1/3} \ln\ln(p)^{(1-1/3)}\right). \qquad (17)$$

В табл. 1 наведені значення складності криптоаналізу генератора для першого методу, тобто при

використанні елементів простого поля Галуа та наступному їх гешуванні. Аналіз цих даних підтверджує високу захищеність ДГВЧ від криптоаналізу у обох випадках.

Таблиця 1

Складність дискретного логарифмування та знаходження прообразу в полі

Метод \ p		2^{256}	2^{1024}	2^{2048}	2^{4096}
n=160	I_{Γ_1}	$1{,}14\cdot10^{62}$	$9{,}9\cdot10^{73}$	$9{,}17\cdot10^{82}$	$5{,}69\cdot10^{94}$
	I_{Γ_2}	$9{,}44\cdot10^{37}$	$8{,}19\cdot10^{49}$	$7{,}58\cdot10^{58}$	$4{,}71\cdot10^{70}$
n=256	I_{Γ_1}	$9{,}04\cdot10^{90}$	$7{,}85\cdot10^{102}$	$7{,}26\cdot10^{111}$	$4{,}51\cdot10^{123}$
	I_{Γ_2}	$2{,}65\cdot10^{52}$	$2{,}3\cdot10^{64}$	$2{,}13\cdot10^{73}$	$1{,}32\cdot10^{85}$
n=384	I_{Γ_1}	$3{,}07\cdot10^{129}$	$2{,}67\cdot10^{141}$	$2{,}47\cdot10^{150}$	$1{,}53\cdot10^{162}$
	I_{Γ_2}	$4{,}9\cdot10^{71}$	$4{,}25\cdot10^{83}$	$3{,}93\cdot10^{92}$	$2{,}44\cdot10^{104}$
n=512	I_{Γ_1}	$1{,}04\cdot10^{168}$	$9{,}09\cdot10^{179}$	$8{,}41\cdot10^{188}$	$5{,}22\cdot10^{200}$
	I_{Γ_2}	$9{,}04\cdot10^{90}$	$7{,}85\cdot10^{102}$	$7{,}26\cdot10^{111}$	$4{,}51\cdot10^{123}$

Таким чином при застосуванні гешування навіть при одномодульному перетворенні забезпечується експоненційна складність визначення ключа генератора, тобто для випадку (16).

Вирішення задачі оцінки складності дискретного логарифмування для багатомодульного перетворення носить специфічний характер і подається окремо.

Висновки

1. На нинішній час розробленоо ряд методів та на їх основі засобів формування ПВП. Їх особливістю є те, що вони будуються, як правило, для двійкової основи $m = 2$. На наш погляд, важливою і необхідною є задача розробки методів і засобів генерування ПВП із необхідними властивостями випадковості та довільною (певною) основою алфавіту. В якості найбільш перспективного, на наш погляд, класу таких перетворень необхідно назвати клас багатомодульних перетворень.

2. Проведені експериментальні дослідження показали необхідність уточнення вимог до взаємних властивостей простого числа p – першого модуля та інших модулів – $p_1, p_2, \ldots, p_{k-1}, m$. Уточнення, в першу чергу, відноситься до модулів $p_1, p_2, \ldots, p_{k-1}, m$ та їх співвідношеннями із модулем p, що наведено в теоремі 1.

3. Детермінований генератор випадкових чисел (ДГВЧ), що функціонує згідно багатомодульного перетворення на основі (1) забезпечує генерування детермінованих випадкових (псевдовипадкових) символів (цілих чисел) з періодом повторення $p-1$, рівноймовірно і з певною основою алфавіту m, за умови, що $p_1 | p-1$, а $m | p_1 - 1$.

4. Для успішного криптоаналізу генератора необхідно спочатку вирішити дискретне логарифмічне рівняння та знайти елемент – прообраз. В цьому випадку спочатку необхідно знайти прообраз відповідного елемента поля A_i зі складністю $I_{ПР}$, а потім вирішити дискретне логарифмічне рівняння зі складністю $I_{ДЛ}$.

Список літератури

1. Потий А.В. Метод многомодульного преобразования чисел / А.В. Потий // Обработка информации и обеспечение надежности систем управления. Сб. науч. тр. – Х.: НАНУ, ПАНИ, ХВУ, 1997. – С. 63-68.

2. Андерсон, Джеймс А. Дискретная математика и комбинаторика. – М.: Изд. дом «Вильямс», 2003 – 960с.

3. Горбенко Ю.І. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика / Ю.І. Горбенко, І.Д. Горбенко. – Х.:. Форт. 2010. – 593 с.

Надійшла до редколегії 9.02.2011

Рецензент: канд. техн. наук, доц. Г.З. Халімов, Харківський національний університет радіоелектроніки.

СВОЙСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ГЕНЕРИРУЕМЫХ НА ОСНОВЕ МНОГОМОДУЛЬНЫХ ПРЕОБРАЗОВАНИЙ В ПОЛЯХ ГАЛУА

Т.А. Гриненко, Ю.И. Горбенко

Определяются условия существования псевдослучайных последовательностей с равновероятным распределением символов m-ичного алфавита в классе многомодульных преобразований. Даются оценки нижних границ необратимости.

Ключевые слова: *псевдослучайная последовательность, многомодульное преобразование, поле Галуа, необратимость.*

PROPERTIES OF PSEUDO-RANDOM SEQUENCES GENERATED ON THE BASIS OF MULTI-CONGRUENCE TRANSFORMATION IN GALOIS FIELDS

T.O. Grinenko, Yu.I. Gorbenko

There are determined existence conditions of pseudo-random sequences with uniform distribution of symbols over m-ary alphabet in class of multi-congruence transformations. There are given estimates of irreversibility lower bounds.

Keywords: *pseudorandom sequence, multi-congruence transformation, Galois field, irreversibility.*