УДК 681.324.067

Т.О. Гріненко

Харківський національний університет радіоелектроніки, Харків

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НЕРОЗРІЗНЮВАНОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ЩО ГЕНЕРУЮТЬСЯ НА ОСНОВІ БАГАТОМОДУЛЬНИХ ПЕРЕТВОРЕНЬ

Реалізовано та досліджено по критерію нерозрізнюваності чотири типи детермінованих генераторів випадкових послідовностей, що базуються на методі багатомодульного перетворення чисел та гешуванні.

Ключові слова: *багатомодульне перетворення, гешування, псевдовипадкова послідовність, нерозрізнюваність, детермінований генератор випадкових послідовностей.*

Вступ

В [1, 2] запропоновано методи генерування псевдовипадкових послідовностей (ПВП) на основі багатомодульних перетворень в скінченних полях $GF(p)$ та $GF(p^n)$. Однак використання таких послідовностей можливо тільки при забезпеченні гарних властивостей нерозрізнюваності. Причому під нерозрізнюваністю розуміється степінь схожості ПВП на фізично випадкову послідовність. Основні вимоги до таких послідовностей з точки зору нерозрізнюваності викладені в [3].

Метою статті є отримання оцінок відносно властивостей нерозрізнюваності ПВП, що генеруються на основі багатомодульних перетворень в скінчених полях Галуа $GF(p)$ та $GF(p^n)$, вихідні значення яких гешуються.

Розглядаються чотири типи детермінованих генераторів випадкових чисел (ДГВЧ). Перший – ДГВЧ в полі $GF(p)$ без гешування, другий – ДГВЧ в $GF(p)$ з гешуванням, третій – ДГВЧ в полі $GF(p^n)$ без гешування, четвертий – ДГВЧ в $GF(p^n)$ з гешуванням згідно [2].

1. ДГВЧ з багатомодульним перетворенням в полі $GF(p)$

Дані, що використовувалися при реалізації ДГВЧ, наведені нижче. Всього було реалізовано 10 ДГВЧ з різними вхідними параметрами (табл. 1).

Параметри ДГВЧ без гешування.

Значення першого модуля p розміром 1024 біти було обрано зі стандарту ISO/IEC 9796-3 [4], причому для всіх реалізацій одне й те ж саме:

p=ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece65381ffffffffffffffff.

Значення другого модуля p_1 (160 біт) було обрано також зі стандарту ISO/IEC 9796-3 [4] для всіх реалізацій одне й те ж, а саме:

p_1=ffd5d55fa9934410d3eb8bc04648779f13174945.

Значення третього модуля було обрано для всіх реалізацій одне й те ж саме, тобто основа алфавіту $m = 2$.

Значення первісного елементу θ (1023 біт) було обрано зі стандарту ISO/IEC 9796-3 [4] для всіх реалізацій одне й те ж саме:

θ =7fffffffffffffffe487ed5110b4611a62633145c06e0e68948127044533e63a0105df531d89cd9128a5043cc71a026ef7ca8cd9e69d218d98158536f92f8a1ba7f09ab6b6a8e122f242dabb312f3f637a262174d31bf6b585ffae5b7a035bf6f71c35fdad44cfd2d74f9208be258ff324943328f67329c0ffffffffffffffff.

Значення ключа генератора k для всіх реалізацій було генероване випадково за умови $k = 1 \div p - 1$. Значення параметрів ДГВЧ в табл. 1.

Параметри ДГВЧ з гешуванням: 5 ДГВЧ це реалізація 3 ДГВЧ з гешуванням за допомогою SHA-1, 6 – реалізація 4 ДГВЧ з гешуванням за допомогою SHA-1, 7 – реалізація 1 ДГВЧ з гешуванням за допомогою SHA-256, 8 – реалізація 1 ДГВЧ з гешуванням за допомогою SHA-384, 9 – реалізація 2 ДГВЧ з гешуванням за допомогою SHA-384, 10 – реалізація 1 ДГВЧ з гешуванням за допомогою SHA-512. Результати експериментальних досліджень цих генераторів наведені в табл. 2 та табл. 3.

2. ДГВЧ з перетвореннями в полі $GF(p^n)$

Всього було реалізовано 8 ДГВЧ з різними вхідними параметрами.

Значення першого модуля $f_1(x)$ було обрано зі стандарту ДСТУ 4145 [5] для всіх реалізацій одне й те ж саме:

Таблиця 1

Параметри ДГВЧ в $GF(p)$, що були використані при тестуванні

Реалізація ДГВЧ	Геш	Розмір першого модуля p, біт	Розмір другого модуля p_1, біт	Значення третього модуля m	Розмір θ, біт	Значення ключа k, 128 біт
1	–	1024	160	2	1023	e6894898f9976ba42761f201cc2ff016
2	–	1024	160	2	1023	84b1c668a99815a269eb15fc87315efc
3	–	1024	160	2	1023	f4bf155fa99f25a259ebf5f1f73f5ef1
4	–	1024	160	2	1023	44b4554a541473419942eb45a2595e41
5-SHA-1 (3)	+	1024	160	–	1023	f4bf155fa99f25a259ebf5f1f73f5ef1
6-SHA-1 (4)	+	1024	160	–	1023	44b4554a541473419942eb45a2595e41
7-SHA-256 (1)	+	1024	160	–	1023	e6894898f9976ba42761f201cc2ff016
8-SHA-380 (1)	+	1024	160	–	1023	e6894898f9976ba42761f201cc2ff016
9-SHA-380 (2)	+	1024	160	–	1023	84b1c668a99815a269eb15fc87315efc
10-SHA-512 (1)	+	1024	160	–	1023	e6894898f9976ba42761f201cc2ff016

$$f_1(x) = x^{431} + x^5 + x^3 + x + 1.$$

Значення другого модуля $f_2(x)$ було обрано зі стандарту ДСТУ 4145 [5] для всіх реалізацій одне й те ж саме:

$$f_2(x) = x^{163} + x^7 + x^6 + x^3 + x + 1.$$

Значення третього модуля $f_3(x)$ було обрано зі стандарту ДСТУ 4145 [5] для всіх реалізацій одне й те ж саме:

$$f_3(x) = 2^8.$$

Значення первісного елементу θ було обрано зі стандарту ДСТУ 4145 [5] для всіх реалізацій одне й те ж саме:

$$\theta = x^{425} + x^{424} + x^{423} + x^{422} + x^{419} + x^{418} + x^{417} + x^{412} + x^{406} + x^{403} + x^{400} + x^{395} + x^{394} + x^{393} + x^{392} + x^{390} + x^{389} + x^{387} + x^{385} + x^{382} + x^{381} + x^{380} + x^{375} + x^{371} + x^{370} + x^{369} + x^{368} + x^{367} + x^{366} + x^{361} + x^{358} + x^{357} + x^{355} + x^{354} + x^{352} + x^{351} + x^{350} + x^{349} + x^{348} + x^{347} + x^{346} + x^{345} + x^{343} + x^{339} + x^{338} + x^{333} + x^{332} + x^{331} + x^{330} + x^{328} + x^{325} + x^{322} + x^{321} + x^{320} + x^{319} + x^{318} + x^{314} + x^{311} + x^{310} + x^{309} + x^{308} + x^{307} + x^{304} + x^{302} + x^{299} + x^{298} + x^{297} + x^{294} + x^{293} + x^{291} + x^{288} + x^{280} + x^{277} + x^{276} + x^{274} + x^{271} + x^{270} + x^{268} + x^{266} + x^{264} + x^{263} + x^{261} + x^{260} + x^{259} + x^{258} + x^{257} + x^{256} + x^{255} + x^{254} + x^{253} + x^{252} + x^{251} + x^{248} + x^{247} + x^{243} + x^{239} + x^{238} + x^{236} + x^{235} + x^{231} + x^{230} + x^{228} + x^{225} + x^{223} + x^{219} + x^{217} + x^{215} + x^{213} + x^{211} + x^{210} + x^{209} + x^{207} + x^{205} + x^{203} + x^{202} + x^{201} + x^{199} + x^{198} + x^{196} + x^{195} + x^{194} + x^{193} + x^{191} + x^{188} + x^{186} + x^{185} + x^{184} + x^{182} + x^{180} + x^{179} + x^{176} + x^{173} + x^{172} + x^{170} + x^{169} + x^{167} + x^{166} + x^{162} + x^{161} + x^{158} + x^{157} + x^{155} + x^{153} + x^{152} + x^{151} + x^{149} + x^{147} + x^{146} + x^{142} + x^{140} + x^{137} + x^{136} + x^{134} + x^{133} + x^{131} + x^{129} + x^{128} + x^{124} + x^{123} + x^{119} + x^{117} + x^{115} + x^{114} + x^{113} + x^{109} + x^{107} + x^{106} + x^{104} + x^{103} + x^{102} + x^{97} + x^{96} + x^{92} + x^{89} + x^{87} + x^{86} + x^{83} + x^{81} + x^{78} + x^{75} + x^{72} + x^{69} + x^{68} + x^{64} + x^{60} + x^{58} + x^{57} + x^{56} + x^{55} + x^{54} + x^{52} + x^{51} + x^{49} + x^{47} + x^{45} + x^{42} + x^{38} + x^{37} + x^{35} + x^{32} + x^{31} + x^{30} + x^{26} + x^{25} + x^{22} + x^{15} + x^{14} + x^{11} + x^9 + x^7 + x^6 + x^5 + x^4 + x + 1.$$

Значення ключа генератора k було генероване випадково за умови $k = 1 \div p^n - 1$.

1 – ДГВЧ в $GF(p^n)$: $k = x^{207} + x^{206} + x^{205} + x^{204} + x^{203} + x^{202} + x^{201} + x^{200} + x^{199} + x^{198} + x^{197} + x^{196} + x^{195} + x^{194} + x^{193} + x^{192} + x^{187} + x^{186} + x^{185} + x^{183} + x^{182} + x^{181} + x^{179} + x^{177} + x^{174} + x^{173} + x^{172} + x^{171} + x^{165} + x^{160} + x^{129} + x^{128} + x^{122} + x^{120} + x^{119} + x^{117} + x^{116} + x^{115} + x^{114} + x^{113} + x^{112} + x^{111} + x^{109} + x^{104} + x^{101} + x^{98} + x^{82} + x^{81} + x^{80} + x^{77} + x^{75} + x^{74} + x^{73} + x^{72} + x^{71} + x^{70} + x^{69} + x^{68} + x^{67} + x^{65} + x^{64} + x^4 + x^2 + 1.$

2 – ДГВЧ в $GF(p^n)$: k = 0xFFFF 0EEA7821 00000003 05bfa124 00072FFB 00000007 00000015.

3 – ДГВЧ в $GF(p^n)$: k =0x151 1596FBBC 47F9B44C ADBC8541 9841BACD FF841632 001F589F 0EEA7821 0034814F 05BFA124 02F846FB 07894ABC 05519584.

4 – ДГВЧ в $GF(p^n)$: k = 0x3CE 10490F6A 708FC26D FE8C3D27 C4F94E69 0134D5BF F988D8D2 8AAEAEDE 975936C6 6BAC536B 18AE2DC3 12CA4931 17DAA469 C640CAF3.

Параметри ДГВЧ в $GF(p^n)$ з гешуванням:

5 – це реалізація 2 ДГВЧ в $GF(p^n)$ з гешуванням за допомогою SHA-384, 6 – за допомогою SHA-160, 7 – за допомогою SHA-256, 8 – за допомогою SHA-512.

Дані експериментальних досліджень цих генераторів наведені в табл. 2 та табл. 3.

Для тестування розроблених ДГВЧ використовувалася методика NIST STS, рекомендована Національним інститутом по стандартизації й технологіям США [7]. Пакет NIST STS містить у собі 16 статистичних тестів.

Таблиця 2

Результати тестування ПВП на нерозрізнюваність за правилом 1

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
1-ДГВЧ GF(p)	136 (71,95%)	189 (100%)
2-ДГВЧ GF(p)	124 (65,6%)	189 (100%)
3-ДГВЧ GF(p)	140 (74,07%)	189 (100%)
4-ДГВЧ GF(p)	130 (68,78%)	189 (100%)
5-SHA-1 (3)	128 (67,72%)	189 (100%)
6-SHA-1 (4)	129 (68,25%)	189 (100%)
7-SHA-256 (1)	129 (68,25%)	189 (100%)
8-SHA-384 (1)	143 (75,66%)	189 (100%)
9-SHA-384 (2)	130 (68,78%)	189 (100%)
10-SHA-512 (1)	122 (64,55%)	189 (100%)
1-ДГВЧ $GF\left(p^n\right)$	138 (73%)	189 (100%)
2-ДГВЧ $GF\left(p^n\right)$	132 (69,84%)	189 (100%)
3-ДГВЧ $GF\left(p^n\right)$	126 (66,67%)	189 (100%)
4-ДГВЧ $GF\left(p^n\right)$	134 (70,8%)	189 (100%)
5-SHA-384 2-ДГВЧ $GF\left(p^n\right)$	139 (73,5%)	189 (100%)
6-SHA-160 2-ДГВЧ $GF\left(p^n\right)$	130 (68,78%)	189 (100%)
7-SHA-256 2-ДГВЧ $GF\left(p^n\right)$	131 (69,31%)	189 (100%)
8-SHA-512 2-ДГВЧ $GF\left(p^n\right)$	128 (67,72%)	189 (100%)

Таблиця 3

Результати тестування ПВП на нерозрізнюваність за правилом 2

Генератор	Кількість тестів, у яких значення ймовірності $P \le 0,01$	Кількість тестів, у яких значення ймовірності $P \le 0,001$
BBS	0	0
1-ДГВЧ GF(p)	4	0
2-ДГВЧ GF(p)	3	0
3-ДГВЧ GF(p)	4	0
4-ДГВЧ GF(p)	0	0
5-SHA-1 (3)	2	0
6-SHA-1 (4)	2	0
7-SHA-256 (1)	2	0
8-SHA-384 (1)	1	0
9-SHA-384 (2)	0	0
10-SHA-512 (1)	2	0
1-ДГВЧ $GF\left(p^n\right)$	0	0
2-ДГВЧ $GF\left(p^n\right)$	4	0
3-ДГВЧ $GF\left(p^n\right)$	2	0
4-ДГВЧ $GF\left(p^n\right)$	1	0
5-SHA-384 2-ДГВЧ $GF\left(p^n\right)$	1	0
6-SHA-160 2-ДГВЧ $GF\left(p^n\right)$	1	0
7-SHA-256 2-ДГВЧ $GF\left(p^n\right)$	1	0
8-SHA-512 2-ДГВЧ $GF\left(p^n\right)$	1	0

Ці тести використовуються для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, що генерувались не детермінованими або ДГВЧ.

По сукупності результатів всіх тестів приймається рішення про те, чи буде задана послідовність нулів і одиниць «випадковою» чи ні.

З використанням методики NIST STS було здійснено тестування псевдовипадкових послідовностей, а також проведене порівняння властивостей цих послідовності із властивостями ПВП генератора псевдовипадкових бітів BBS (тестова вибірка, рекомендована NIST).

В табл. 2 наводяться дані по проходженню ПВП тестів за правилом 1 [1]. При цьому дані відносно генератора BBS взяті для контролю [7].

В табл. 3 представлені зведені результати по проходженню генераторами тестів за правилом 2 [6, 7]. В табл. 4 наведено результати експериментальної оцінки швидкості формування ПВП для різних алгоритмів (Мб/сек).

На рис. 1 та рис. 2, в якості прикладів, наведені фазові портрети нерозрізнюваності, що отримані і з використанням методики тестування NIST STS [6, 7]. Їх аналіз дозволяє зробити висновок про високу якість нерозрізнюваності (випадковості).

Таблиця 4

Результати експериментальної оцінки швидкості формування ПВП

ДГВЧ	Без гешування	SHA-1	SHA-256	SHA-384	SHA-512
ДГВЧ в $GF(p)$	0,1	8,3	10,4	11,4	12,7
ДГВЧ в $GF(p^n)$	0,003	0,052	0,089	0,131	0,173

Рис. 1. Результати експериментальних досліджень ДГВЧ 8-SHA-384 (1)

Рис. 2. Результати експериментальних досліджень ДГВЧ 5-SHA-384 2-ДГВЧ $GF(p^n)$

Проведемо також аналіз ПВП згідно вимог належності класам К1- К4 AIS 20 [3]. В табл. 5 наведені в узагальненому вигляді вимоги, які ними висуваються. Також відмітимо, що класи є ієрархічно залежними, тобто кожен наступний повністю включає в себе попередній та доповнює своїми новими вимогами. Наведені вище результати досліджень дозволяють зробити висновок про те, що ПВП багатомодульних перетворень можуть застосовуватись практично у більшості криптографічних додатків. Обмеження можуть виникати тільки із-за складності перетворень (швидкодії).

Таблиця 5

Порівняння функціональних класів К1 – К4

Функціональний клас	Вимоги до ДГВП	Криптографічні системи, в яких застосовуються ДГВП такого класу
К1	К1(i)	Інтерактивні протоколи
К2	К1(i)+ К2(ii)	Потокові шифри
К3	К1(i)+ К2(ii)+ К3(iii)+ К3(iv)	Генерація ключів, Генерація цифрового підпису DSS (секретний ключ x або випадкове число k), Генерація паролів.
К4	К1(i)+ К2(ii)+ К3(iii)+ К3(iv)+ К4(v)	Генерація ключів, Генерація цифрового підпису DSS (секретний ключ x або випадкове число k), Генерація сеансових ключів для симетричних криптографічних механізмів, Генерація паролів.

Вказані вимоги встановлюють всі рівні захищеності, як від найменшого (використання ДГВП як лічильника), так і найвищого (аналітик, навіть при знанні певних внутрішніх станів генератора, не може скомпрометувати усю послідовність). Причому методика тестування AIS 20 може застосовуватись як в реальному часі, так і в процесі досліджень, а також для технологічного тестування.

Висновки

На нинішній час розроблено 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.

ДГВЧ, що функціонує згідно багатомодульного перетворення, забезпечує генерування псевдовипадкових символів (цілих чисел) з періодом повторення $p-1$, рівно ймовірно і з певною основою алфавіту m.

Достатньо велика статистика досліджень дозволяє зробити висновок, що кращими відносно нерозрізнюваності є генератори багатомодульних перетворень, у яких передостанні елементи гешуються (табл. 2, генератори 5 – 10 в $GF(p)$, генератори 5 – 8 в $GF(p^n)$). При цьому, якість нерозрізнюваності практично не залежить від параметрів функції гешування класу SHA функцій.

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. Гріненко Т.О. Метод генерування псевдовипадкових послідовностей на основі багатомодульних перетворень в скінчених полях / Т.О. Гріненко, Ю.І. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 9. № 1. – С. 35-41.

3. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for Deterministic random number generator. 1999.

4. ISO/IEC 9796-3:2006 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.

5. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння».

6. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. April 2000 [Електронний ресурс]. – Режим доступу до ресурсу: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

7. Потий А.В. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / А.В. Потий, С.Ю. Орлова, Т.А. Гриненко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вып. 2. – С. 206–214.

Надійшла до редколегії 7.04.2011

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

ИССЛЕДОВАНИЕ СВОЙСТВ НЕРАЗЛИЧИМОСТИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ГЕНЕРИРУЕМЫХ НА ОСНОВЕ МНОГОМОДУЛЬНЫХ ПРЕОБРАЗОВАНИЙ

Т.А. Гриненко

Реализованы и исследованы по критерию неразличимости четыре типа детерминированных генераторов случайных последовательностей, основанных на методе многомодульного преобразования чисел и хешировании.

Ключевые слова: *многомодульное преобразование, хеширование, псевдослучайная последовательность, неразличимость, детерминированный генератор случайных последовательностей.*

RESEARCH OF INDISTINGUISHABILITY PROPERTIES OF PSEUDORANDOM SEQUENCES GENERATED BY MULTI-CONGRUENCE TRANSFORMATION

T.A. Grinenko

There are implemented and researched by the indistinguishability criterion the four types of deterministic random sequence generators based on the method of multi-congruence transformation of numbers and hashing.

Keywords*: multi-congruence transformation, hashing, pseudorandom sequence, indistinguishability, deterministic generator of random sequences.*