

Н. М. Лужецька, С. С. Войтусік, А. Я. Горпенюк
Національний університет “Львівська політехніка”,
¹кафедра безпеки інформаційних технологій”,
²кафедра захисту інформації

ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОБЧИСЛЮВАЧАХ ІРРАЦІОНАЛЬНИХ ЧИСЕЛ

© Лужецька Н. М., Войтусік С. С., Горпенюк А. Я., 2015

Подано результати синтезу та дослідження генераторів псевдовипадкових чисел на обчислювачах квадратного кореня з простого числа, чисел p і e . Показано, що такі генератори мають добрі статистичні характеристики роботи. Запропоновано алгоритми обчислення таких чисел, які дають змогу будувати високошвидкісні генератори псевдовипадкових чисел.

Ключові слова: генератор псевдовипадкових чисел, криптографія, криптоаналіз, ірраціональне число.

The results of pseudorandom numbers generators synthesis and research are presented based on the calculators of square root of a prime number, numbers p and e . These generators are shown to have qualitative statistical properties. The proposed algorithms for computing these numbers allows us to build high speed generator.

Key words: pseudorandom number generator, cryptography, cryptanalysis, irrational number.

Вступ

Сьогодні криптографічні методи та алгоритми дають змогу вирішувати такі завдання захисту інформації: забезпечення конфіденційності, незаперечення авторства, перевірка оригінальності (аутентифікація), забезпечення цілісності інформації тощо [1]. Значно розширилась також область застосування випадкових та псевдовипадкових чисел у захисті інформації. Сьогодні це не тільки продукування надійних криптографічних ключів, але й область імітаційного моделювання і, особливо, область криптографічних протоколів, де випадкові і псевдовипадкові числа є потужним інструментом запобігання деяким небезпечним атакам на протоколи, таким як атака з повторним використанням. Проблеми ефективного генерування довгих випадкових чисел є загальновідомі. При застосуванні замість випадкових псевдовипадкових чисел одним з критичних параметрів останніх є періодичність. Проте не всі генератори псевдовипадкових чисел (ГПВЧ) є періодичні. Зокрема не доведено сьогодні гіпотези про нормальність ірраціональних чисел, що дає підстави сподіватися, що генератори на обчислювачах ірраціональних чисел є неперіодичними. Неперіодичність є важливою властивістю таких генераторів. Однак актуальним є розроблення ефективних алгоритмів обчислення ірраціональних чисел, придатних для побудови ГПВЧ.

Аналіз методів генерування псевдовипадкових чисел

Згідно із Райнером Рюппелом, існує чотири основні підходи до проектування генераторів псевдовипадкових чисел [1]:

- Системно-теоретичний підхід;
- Інформаційно-теоретичний підхід;
- Складнісно-теоретичний підхід;
- Рандомізований підхід.

Більшість сучасних ГПВЧ будують відповідно до системно-теоретичного підходу на основі регістрів зсуву із лінійними зворотними зв'язками. Такі генератори мають високу швидкодію, тому можуть застосовуватися як генератори гамми в поточкових шифрах. В межах складнісно-теоретичного підходу ГПВЧ переважно будують на обчислювачах важкооборотних

криптографічних функцій. Такі генератори повільніші, тому застосовуються для генерування ключів та інших випадкових параметрів тривалого зберігання. Загалом більшість сучасних ГПВЧ апаратно реалізують як цифрові автомати зі скінченною кількістю станів, тому вони принципово періодичні. Разом з тим вимога неперіодичності до згенерованих псевдовипадкових чисел криптографічного застосування і одночасно зростаючі вимоги до довжини ключових параметрів ускладнюють генератори такого типу.

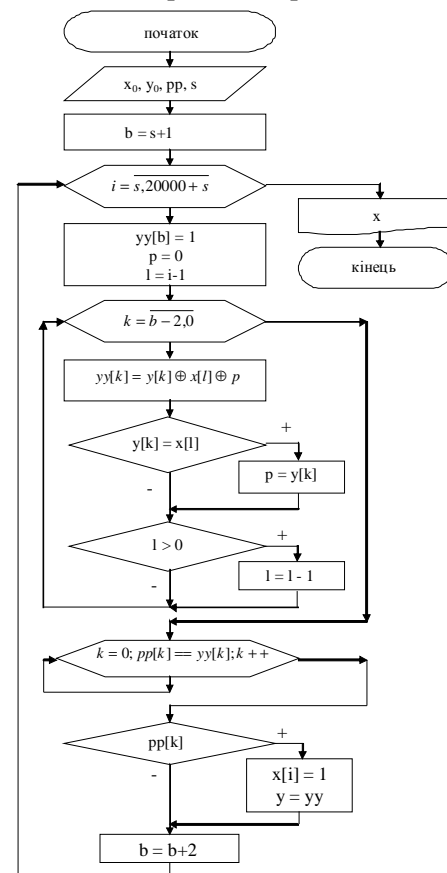
ГПВЧ на обчислювачах ірраціональних чисел

У математиці відома гіпотеза про нормальність ірраціональних та трансцендентних чисел, зокрема чисел π , e , квадратних коренів з простих чисел [2]. Фактично це означає, що послідовність цифр таких чисел становить псевдовипадкову неперіодичну послідовність. Згадана гіпотеза є недоведеною і належить до найвідоміших невирішених математичних задач. Задача обчислення великої кількості розрядів таких чисел дотепер актуальна, а історія спроб розв'язання цієї задачі налічує тисячі років. Найдавнішим відомим ірраціональним числом є квадратний корінь з двійки.

Розглянемо можливість побудови ГПВЧ на обчислювачі квадратного кореня з простого числа. Такий обчислювач повинен розрахувати велику кількість розрядів кореня. Більше того, кожен черговий розряд результату має бути обчислений точно. Інакше властивість псевдовипадковості згенерованої послідовності може бути втрачена. Крім того, розряди квадратного кореня, які стають бітами псевдовипадкової послідовності і можуть застосовуватися в швидких потокових шифрах, мають розраховуватися швидко. Отже, необхідно застосувати швидкий і точний обчислювач “цифра за цифрою”. Відповідно різноманітні методи грубого оцінювання значення квадратного кореня придатні хібащо для розрахунку початкового наближення. Малопридатні також такі методи, як метод обчислення в стовпчик і більшість з наближених числових методів (Герона, хорд, дотичних тощо) через високу складність обчислювальних операцій, яка зростає із збільшенням кількості обчислених розрядів. Метод обчислення в стовпчик дає можливість обчислення результату “цифра за цифрою”. Зручним для побудови обчислювача генератора ПВЧ є метод половинного ділення. За цим методом застосовують доволі прості обчислювальні операції. Він має повільну збіжність, однак є швидким і за певних умов може бути перетворений на метод “цифра за цифрою”.

У роботі [3] запропоновано вдосконалений метод бісекцій для обчислення кореня з простого числа, зручний для побудови ГПВЧ. Суть вдосконалення полягає в тому, що ширину відрізка початкового наближення має дорівнювати цілому степеню двійки. Так отримують точне значення чергового біта результату на кожному кроці алгоритму. Крім того, це дає змогу в алгоритмі половинного ділення відмовитися від контролю за правою межею відрізка локалізації кореня, а також виконувати обчислення середини відрізка простим дописуванням одиниці в черговий біт. Генеруючи послідовність ПВЧ, яка у випадку застосування обчислювача квадратного кореня з простого числа є неперіодичною, ми можемо почати генерацію з будь-якого біта, вибравши початкове наближення відповідно до сформульованого вдосконалення.

За вдосконаленим методом бісекцій було розроблено алгоритм [3] функціонування ГПВЧ на обчислювачі кореня з простого числа (рисунк). Приблизна складність цього алгоритму – одне додавання на один біт результату.



Алгоритм ГПВЧ
на обчислювачі кореня з простого числа

Аналіз методів обчислення числа e показав, що відомі методи обчислення числа e є повільними і трудомісткими. Крім того, ці методи не дають змоги вести обчислення з заданого розряду без обчислення попередніх, що робить проблематичним застосування таких обчислювачів у ГПВЧ, оскільки не передбачає можливості задання якого-небудь ключа генератора у вигляді, наприклад, номера розряду, з якого починається генерування.

Аналіз методів обчислення числа p показує, що тільки два з відомих методів доцільно застосовувати, будуючи ГПВЧ. Це формули Бейлі–Боружейна–Плаффа та Беллара.

Формулу Бейлі–Боружейна–Плаффа (англ. BaileyBorweinPlouffe formula) відкрив у 1997 році Саймон Плафф (англ. Simon Plouffe):

$$p = \sum_{k=0}^{\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right)$$

Ця формула дає змогу обчислити будь-яку конкретну шістнадцяткову або двійкову цифру числа π без обчислення попередніх.

За формулою Беллара обчислюють n -й розряд π у двійковому представленні. Це швидка модифікація (приблизно на 43 % швидша) формули Бейлі–Боружейна–Плуффа. Формулу відкрив французький програміст Фабріс Беллар. Використовується в проєкті розподіленого обчислення числа π PiHex. Формула Беллара має такий вигляд:

$$p = \frac{1}{2^6} \sum_{n=0}^{\infty} \frac{(-1)^n}{2^{10n}} \left(-\frac{2^5}{4n+1} - \frac{1}{4n+3} + \frac{2^8}{10n+1} - \frac{2^6}{10n+3} - \frac{2^2}{10n+5} - \frac{2^2}{10n+7} + \frac{1}{10n+9} \right).$$

Саме формула Беллара є найзручнішою для побудови ГПВЧ на обчислювачі числа p .

Дослідження статистичних характеристик ГПВЧ на обчислювачах ірраціональних чисел

Із застосуванням досліджених алгоритмів обчислення ірраціональних чисел було розроблено програми генерування та визначення статистичних характеристик генераторів ПВЧ на обчислювачах числа π та кореня з простого числа. В програми інтегровано статистичні тести, розроблені для розрахунку статистичних характеристик генераторів відповідно до стандарту FIPS 140-2.

У процесі дослідження аналізували послідовність псевдовипадкових бітів завдовжки 20000 бітів, отриманих розрахунком бітів ірраціональних чисел. При цьому тестували згенеровану послідовність за стандартом FIPS 140-2. Результати тестування статистичних властивостей генераторів наведено у таблиці, де тести серій одиниць подано у верхньому рядку, а тести серій нулів – у нижньому.

Результати тестування статистичних характеристик генераторів

	Монобітний тест	Блоковий тест	Тест серій						Тест довжини серії
			1	2	3	4	5	6	
$\sqrt{7}$	10013	7	2373	1222	611	325	168	152	11
			2477	1284	654	317	178	143	
$\sqrt{19}$	10043	15	2459	1210	607	353	147	159	17
			2499	1273	634	360	154	157	
$\sqrt{29}$	10034	19	2511	1214	665	342	173	125	12
			2529	1222	613	319	135	159	
π	9976	17	2457	1267	659	349	176	148	9
			2499	1219	632	327	159	150	

Прийнятними показниками тестів відповідно до стандарту FIPS 140-2 є такі:

Монобітовий тест $9654 < n1(n2) < 10346$.

Блоковий тест $1,03 < X_3 < 57,4$.

Тест серій

Довжина серії	Необхідний інтервал
1	2267 – 2733
2	1079 – 1421
3	502 – 748
4	223 – 402
5	90 – 223
6	90 – 223

(із збільшенням довжини серії на 1 – кількість серій зменшується приблизно удвічі)

Тест довжин серій

Максимальна довжина серії не повинна перевищувати значення 34.

Аналізуючи результати досліджень розроблених генераторів, наведених у таблиці, доходимо висновку, що статистичні характеристики генераторів ПВЧ на обчислювачах ірраціональних чисел відповідають вимогам стандарту FIPS 140-2. Розробленим і дослідженим генераторам псевдовипадкових чисел на обчислювачах ірраціональних чисел властива висока швидкість генерування завдяки використанню швидких побітових алгоритмів обчислення ірраціональних чисел. Ключовими параметрами таких генераторів є номер біта, з якого починається генерування, а для генератора на обчислювачі кореня з простого числа додатково – просте число, корінь з якого обчислюється.

Висновки

У роботі запропоновано способи побудови генераторів псевдовипадкових чисел на обчислювачах ірраціональних чисел. Важливою перевагою таких генераторів є неперіодичність згенерованого числа. Показано, що сьогодні немає ефективних методів обчислення розрядів числа e , починаючи із заданого розряду. Натомість генератор може бути побудований на обчислювачі числа p за формулами Бейлі–Боружейна–Плаффа та Беллара. Ці формули дозволяють розряд за розрядом розрахувати числа, починаючи із заданого розряду. При цьому номер цього розряду може бути ключовим параметром генератора. Швидкий генератор можна побудувати на обчислювачі квадратного кореня з простого числа. В роботі вдосконалено модифікований алгоритм бісекцій [3], який дозволяє біт за бітом обчислювати корінь із заданого простого числа, починаючи з заданого біта. Ключовими параметрами при цьому можуть бути просте число і номер біта, з якого починається розрахунок.

1. Брюс Шнайер. Прикладная криптография (2-е изд., Протоколы, алгоритмы и исходники на C). – М., Триумф, 2002. 2. Беркович Е. Мировые константы π и e в природе // Журнал “7 искусств”, № 1, декабрь 2009 – <http://7iskusstv.com>, 2010. 3. Горпенюк А. Я., Лужецька Н. М. “Генератор псевдовипадкових чисел на обчислювачі кореня квадратного з простого числа” // Вісник Нац. ун-ту “Львівська політехніка” “Автоматика, вимірювання та керування”. – 2013. – № 753. – С. 45–50.