УДК 621.317

В.С. ПЕТРУШАК, І.В. СТОЛЯРЧУК
Хмельницький національний університет

# АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ФОРМУВАННЯ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ ЧИСЕЛ

*В роботі проаналізовано методи та засоби формування псевдовипадкової послідовності чисел. В результаті аналізу зібрано основні дані для вибору оптимальних засобів формування псевдовипадкової послідовності чисел за основними показниками ефективності.*

*Ключові слова: псевдовипадкова послідовність, генератор псевдовипадкових чисел.*

V.S. PETRUSHAK, I.V. STOLYARCHUK
Khmelnytsky National University

**ANALYSIS THE METHODS AND MEANS OF FORMING PSEUDORANDOM SEQUENCE OF NUMBERS**

*The work analyzes the methods and means of forming pseudorandom sequence of numbers. As a result of collected basic data to select the optimum means of forming pseudorandom sequence numbers in key performance indicators.*

*Keywords: pseudorandom sequence, pseudorandom number generator.*

## Вступ

В умовах стрімкої інформатизації суспільства, широкого застосування засобів обчислювальної техніки та комп'ютерних систем особливу актуальність набувають питання інформаційної безпеки, найбільш складними з яких є необхідність захисту цінної конфіденційної і секретної інформації в державних і приватних підприємствах, в органах і установах державного управління, банківської справи та інших системах. Збільшення обсягів оброблювальних і переданих даних у комп'ютерних системах та мережах вимагає нових підходів до протоколів і механізмів забезпечення безпеки переданих даних.

Незважаючи на широке застосування різних криптографічних алгоритмів на різних рівнях захисту інформаційні системи схильні до різних атак і загроз. Під загрозою розуміють можливий вплив на інформаційну систему, який прямо чи побічно може завдати шкоди її безпеки. [1]

Для забезпечення безпеки комп'ютерних систем критично вважливо мати алгоритми, що задовольняють такому критерію як непередбачуваність. Іншими словами, навіть знаючи алгоритм генератора й всі попередні елементи послідовності, повинне бути максимально трудомістким обчислення наступних елементів.

Для забезпечення захисту від загроз безпеки використовуються різні криптографічні механізми. Для побудови механізмів захисту інформації використовують методи криптографічної обробки інформації. Важливе місце в розвитку сучасних механізмів забезпечення безпеки інформаційних систем і технологій займає використання псевдовипадкових чисел (ПВЧ) і відповідно генераторів псевдовипадкових чисел (ГПВЧ). Вони використовуються для вирішення наступних завдань: хешування інформації, побудови синхронних і само синхронізуючих поточних шифрів, формування ключової інформації і т. д. [2]

Генератор псевдовипадкових чисел (ГПСЧ, англ. Pseudorandom number generator, PRNG) – алгоритм, що генерує послідовність чисел, елементи якої майже незалежні один від одного і підкоряються заданому розподілу (зазвичай рівномірному).

Ці програми та пристрої насправді генерують детерміновані послідовності, які тільки здаються випадковими за своїми властивостями але насправді підпорядковується деякому закону і, як правило, рано чи пізно зациклюється і тому називаються псевдовипадковими послідовностями.

Найважливіша характеристика генератора псевдовипадкових чисел - це інформаційна довжина його періоду, після якого числа будуть або просто повторюватися, або їх можна буде передбачити [4].

## Експериментальна частина

Одним з перших таких методів генерування псевдовипадкових чисел був метод, запропонований в 1946 році Д. фон Нейманом [3].

Основна ідея методу полягає у тому, що ГВЧ формує наступний елемент послідовності на основі попереднього шляхом піднесення його до квадрату і виділення середніх цифр отриманого числа.

Однак він має недоліки:

- якщо який-небудь член послідовності виявиться рівним нулю, то всі наступні члени також будуть нулями;
- послідовності мають тенденцію "зациклюватися", тобто з рештою, утворять цикл, що повторюється нескінченне число раз;
- властивість "зациклюватися" притаманна всім послідовностям, побудованих по рекурентній формулі;

Недоліки методу серединних квадратів обмежують його практичне застосування, хоча раніше до цього методу вдавалися завдяки його простоті.

Метод середин квадратів фон Неймана, як було показано, фактично є порівняно бідним джерелом випадкових чисел. Небезпека полягає в тому, що послідовність прагне ввійти у звичну колію, тобто короткий цикл повторюваних елементів [4].

Іншим методом є так званий лінійний конгруентний спосіб, що був запропонований Д. Х. Лемером в 1948 році. Такий спосіб генерування псевдовипадкових чисел застосовується в простих випадках і не має криптографічної стійкості. Використовується в якості стандартного генератора з багатьма компіляторами.

Основна обчислювальна формула має вигляд:

$$x_{n+1} = (ax_n + c) \bmod m \quad (1)$$

Алгоритм зациклюється з періодом, що не перевищує деякого *m*. Коефіцієнти *a*, *m* і *x(0)* можуть приймати довільні цілі значення, за винятком 0. Параметр *c* може бути також і 0, але в цьому випадку скорочується період повтору. Число ітерацій *m* зазвичай вибирається рівним максимальному значенню типу, що робить непотрібною операцію ділення, яка автоматично виконається при переповненні. Число *a* можна взяти рівним, наприклад, 1664525, *c* - рівним 1013904223. Такий метод часто реалізують в сучасних системах програмування, хоча він майже непридатний у галузі статистики чи криптографії, де вимоги до „випадковості" значно вищі.

Отримана послідовність залежить від вибору стартового числа $x_0$ і при різних його значеннях отримуємо різні послідовності випадкових чисел. У той же час, багато властивостей послідовності $x_j$ визначаються вибором коефіцієнтів у формулі і не залежать від вибору стартового числа. Ясно, що послідовність чисел, що генерується таким алгоритмом, періодична з періодом, що не перевищує $m$.

При реалізації вигідно вибирати $m = 2^e$, де $e$ – число біт у машинному слові, оскільки це дозволяє позбутися від відносно повільної операції приведення по модулю [4].

У 1986 році троє авторів Ленор Блюм, Мануель Блюм і Майкл Шуб запропонували алгоритм генерації псевдовипадкової послідовності, стійкий до зворотних перетворень. Основна рекурентна формула алгоритму має вигляд:

$$x_n = (x_{n-1})^2 \bmod pq \quad (2)$$

де $p$ *і* $q$ – два великих простих числа.

Для підвищення якості отриманої послідовності при наступному кроці обираються не всі біти $x_n$, а лише менші, або навіть біти парності. З отриманих «випадкових бітів» формуються двійкові псевдовипадкові числа довільної розрядності. Однією з особливостей обчислювальної формули є наскрізна можливість обчислити $x_n$ без генерації всіх попередніх членів послідовності.

$$x_n = x_0^{2^n \bmod ((p-1)(q-1))} \bmod pq \quad (3)$$

Даний алгоритм більш вимогливий до обчислювальних ресурсів, але, з іншого боку, має гарні статистичні характеристики.

Цей генератор підходить для криптографії, але не для моделювання, тому що він не достатньо швидкий. Однак, він має надзвичайно високу стійкість, яка забезпечується якістю генератора виходячи з обчислювальної складності задачі факторизації чисел [3].

Не менш цікавим методом утворення псевдовипадкових послідовностей є вихор Мерсенна, який було розроблено в 1997 японськими вченими Макото Мацумото і Такудзі Нісімура. Такий метод забезпечує швидку генерацію високоякісних псевдовипадкових чисел, і був розроблений з урахуванням помилок, знайдених в інших алгоритмах.

Існують що найменше два загальних варіанти алгоритму, що відрізняються лише розміром простого числа Мерсенна. Новітній і найбільш поширений називається Mersenne Twister MT 19937.

Перевагами цього методу є:

- колосальний період ($2^{19937} - 1$);
- рівномірний розподіл в 623 вимірах (для порівняння лінійний конгруентний метод генерує розподіл в 5 вимірах);
- швидка генерація випадкових чисел (в 2-3 рази швидше, ніж стандартні ГПВЧ, що використовують лінійний конгруентний метод);

Разом з тим існують складні алгоритми, що розпізнають послідовність, яка утворюється за допомогою вихору Мерсенна як невипадкову. Це унеможливлює використання вихору Мерсенна в криптографії.

«Вихор» – це перетворення, що забезпечує рівномірний розподіл псевдовипадкових чисел в 623 вимірах. Тому кореляція між послідовними значеннями у вихідній послідовності алгоритму вихору Мерсенна дуже мала.

Інший клас генераторів псевдовипадкових послідовностей заснований на використанні послідовностей Фібоначчі. Класичний приклад такої послідовності {0,1,1,2,3,5,8,13,21,34 ...} – за винятком перших двох її членів, кожний наступний член дорівнює сумі двох попередніх.

Особливості розподілу випадкових чисел, що генеруються лінійним конгруентним алгоритмом, роблять неможливим їх використання в статистичних алгоритмах. У зв'язку з цим лінійний конгруентний

алгоритм поступово втратив свою популярність, і його місце зайняло сімейство алгоритмів Фібоначчі, які можуть бути рекомендовані для використання в алгоритмах побудови псевдовипадкових чисел.

Запропоновано спосіб побудови модифікованого адитивного генератора Фібоначчі, в якому введення додаткової складової в процес додавання, дає змогу формувати псевдовипадкові числа за модулем, що дорівнює ступеню двійки, і тим самим істотно спрощує його апаратну реалізацію у порівнянні з відомими рішеннями, при збереженні високих статистичних характеристик ГПВЧ, побудованих на його основі. При цьому період повторення псевдовипадкової послідовності збільшується на кілька порядків у порівнянні з ГПВЧ на основі класичного генератора Фібоначчі, наприклад, у 15 разів при застосуванні логічної схеми з трьох логічних функцій і у 2290 раз – з семи логічних функцій.

**Висновки**

У теорії ніякий детермінований алгоритм не може генерувати повністю випадкові числа, а тільки апроксимувати деякі властивості випадкових чисел. Тому у принципі будь-який генератор випадкових чисел на практиці завжди є лише генератором псевдовипадкових чисел, проте завдання розробника генератора полягає в тому, щоб зробити алгоритм якомога більш варіаційним.

Розглянувши основні методи генерування псевдовипадкових чисел найкращими характеристиками володіє вихор Марсенна та метод Фібоначчі, адже випадкові числа, отримані за допомогою таких методів, мають гарні статистичні властивості, причому всі біти випадкового числа рівнозначні за статистичних властивостей. У методі лінійно конгруентної послідовності ілюструється той факт, що така послідовність завжди утворює петлі, тобто обов'язково існує цикл, що повторюється нескінченне число разів (перетворить кінцеву множину саму в себе). Метод середин квадратів фон Неймана має порівняно вузький спектр випадкових чисел. Небезпека полягає в тому, що послідовність прагне ввійти у звичну колію, тобто короткий цикл повторюваних елементів. Наприклад, кожна поява нуля як числа послідовності приведе до того, що всі наступні числа також будуть нулями.

**Література**

1. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник / В.В. Поповский, А.В. Персиков; Харьковский национальный университет радиоэлектроники. Х.: "Компания Смит", 2006. 238 с.

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. Конгруентний метод формування псевдовипадкових чисел – Режим доступу.: http://cppstudio.com/uk/post/1296/.

4. Генерація випадкових чисел – Режим доступу.: https://uk.wikipedia.org/wiki/Генерація_випадкових_чисел.

Рецензія/Peer review : 1.12.2015 р. Надрукована/Printed : 16.2.2016 р.
Рецензент: д.т.н., проф. Ройзман В.П.