Генератор випадкових чисел з апаратним джерелом ентропії

Маргарита Геннадіївна Долотій[*], Павло Володимирович Мерзликін[#]
Кафедра інформатики та прикладної математики, Криворізький державний педагогічний університет, пр. Гагаріна, 54, м. Кривий Ріг, 50086, Україна
mdolotiy@gmail.com[*], linuxoid@i.ua[#]

Анотація. *Метою дослідження* є створення бібліотеки для генерації випадкових чисел із використанням аудіоадаптера як джерела ентропії. Для досягнення мети слід розв'язати такі *задачі дослідження*:

– проаналізувати актуальні підходи до генерації послідовностей випадкових чисел;

– порівняти наявні реалізації генераторів випадкових чисел;

– висунути функціональні вимоги до майбутнього програмного забезпечення;

– спроектувати алгоритми та структури даних;

– обрати інструменти розробки;

– створити програмну реалізацію бібліотеки для генерації випадкових чисел із апаратним джерелом ентропії.

Об'єктом дослідження є генерація випадкових чисел. *Предметом дослідження* є генератор випадкових чисел із апаратним джерелом ентропії. Новизна роботи полягає в тому, що в її рамках створено бібліотеку для операційних систем сімейства Microsoft Windows для генерації випадкових чисел на основі шумів аудіоадаптеру. В ході роботи проведено експериментальні дослідження для виявлення типу розподілу згенерованих чисел. *Результати дослідження* можуть бути використані в галузях криптографії, комп'ютерного моделювання та інших сферах, що потребують послідовності випадкових чисел високої якості.

Ключові слова: генератор випадкових чисел; джерело ентропії; статистичний критерій; закон розподілу.

M. G. Dolotii[*], P. V. Merzlykin[#]. The random number generator with hardware source of entropy

Abstract. The *aim* of this study is to create a library to generate random numbers using the audio adapter, as a source of entropy.

To achieve the goal the following *objectives of the study* should be solved:

– to analyse current approaches to random numbers sequences generation;

– to compare the existing implementations of random number generators;

– to propose the functional requirements for future software;

– to design algorithms and data structures;

– to choose the development tools;

– to create a software implementation of a library for generating random numbers with a hardware source of entropy.

The object of study is the generation of random numbers. *The subject of study* is the random number generator with hardware source of entropy. The novelty of this work lies in the fact that the library for Microsoft Windows operating systems for random numbers generation, based on the noise of audio adapter, has been created. Within the framework of the research the examination of generated numbers distribution has been carried out. *The results of the study* can be used in the areas of cryptography, computer simulation, and other fields that require sequences of high quality random numbers.

Keywords: random number generator; source of entropy; test statistic; probability distribution.

Affiliation: Department of Computer Science and Applied Mathematics, Kryvyi Rih State Pedagogical University, 54, Gagarin avenue, Kryvyi Rih, 50086, Ukraine.

E-mail: mdolotiy@gmail.com*, linuxoid@i.ua#.

За останні роки розвиток обчислювальної техніки досяг меж, які здавалися неможливими ще якесь десятиріччя тому. Повсякденне її використання стимулюється розширенням сфери можливих застосувань, а масовість реалізацій призводить до доступності з погляду цінового фактору.

Досить часто в нашому житті виникають ситуації, коли необхідно одержувати випадкові або псевдовипадкові числові послідовності. Найчастіше дана задача виникає при організації різного роду ігрових ситуацій, при реалізації криптографічних алгоритмів та комп'ютерних моделей.

Генерування випадкових послідовностей із заданим ймовірнісним законом та перевірка їх адекватності – одні з найважливіших проблем сучасної криптології. Наукова і практична значимість цієї проблеми настільки велика, що їй присвячені окремі монографії в області криптології, організовуються розділи в наукових журналах «Journal of Cryptology», «Cryptologia» і спеціальні засідання на міжнародних наукових конференціях «Eurocrypt», «Asiacrypt», «Crypto» та ін.

У даний час попит на генератори випадкових послідовностей із заданими ймовірнісними розподілами, а також на самі випадкові послідовності настільки зріс, що за кордоном з'явилися науково-виробничі фірми, які займаються виробництвом і продажем великих масивів випадкових чисел. Наприклад, з 1996 р. у світі поширюється компакт-диск «The Marsaglia random number CDROM», який містить

4,8 млрд. «істинно випадкових» біт [1].

Таким чином, тема дослідження видається актуальною. Робота присвячена створенню генератора випадкових чисел, що використовує як джерело ентропії шуми звукової карти. Генерація має відбуватися в межах деякого діапазону. Також генератор має створювати таку генерацію, що попередить зламування даного набору чисел, тобто прогнозування наступного набору за значенням попереднього.

У ході дослідження було проведено порівняльний аналіз генераторів випадкових чисел. В результаті було виявлено, що використовувати стандартні детерміновані генератори псевдовипадкових чисел, які надаються багатьма бібліотеками, є недоцільним через те, що існує ризик повторення й зламування генерованої послідовності.

Виходячи з результатів порівняльного аналізу вибір було зроблено на користь генератора випадкових чисел із апаратним джерелом ентропії. Загалом створена бібліотека випадкових чисел має задовольняти таким вимогам:

– генерувати статистично незалежні випадкові числа, рівномірно розподілені в інтервалі [0, 1];

– мати можливість відтворювати задані розподіли випадкових чисел;

– затрати ресурсів процесора на роботу генератора повинні бути мінімальними.

За джерело ентропії зручно приймати шуми звукової карти, адже фактично неможливо точно відтворити записаний звук. Тому можна стверджувати, що генератор на основі шумів звукової карти є більш захищеним від зламування.

Програмну реалізацію генератора було створено засобами Windows API, через те, що це найбільш низькорівневий документований інтерфейс взаємодії з операційною системою, який забезпечує однаковий спосіб взаємодії незалежно від моделі звукового адаптера.

Тестування бібліотеки генерації випадкових чисел показало, що згенеровані послідовності описуються законом рівномірного розподілу (рис. 1).

У майбутньому планується реалізувати можливість зведення генерованих послідовностей до обраних розподілів, підтримку багатопоточності, взаємодію з іншими апаратними джерелами ентропії.

Основним результатом роботи є бібліотека для генерації випадкових чисел з використанням аудіоадаптера в ролі апаратного джерела ентропії, що може бути використана для розробки програмного забезпечення, яке має потребу в якісних послідовностях випадкових чисел.

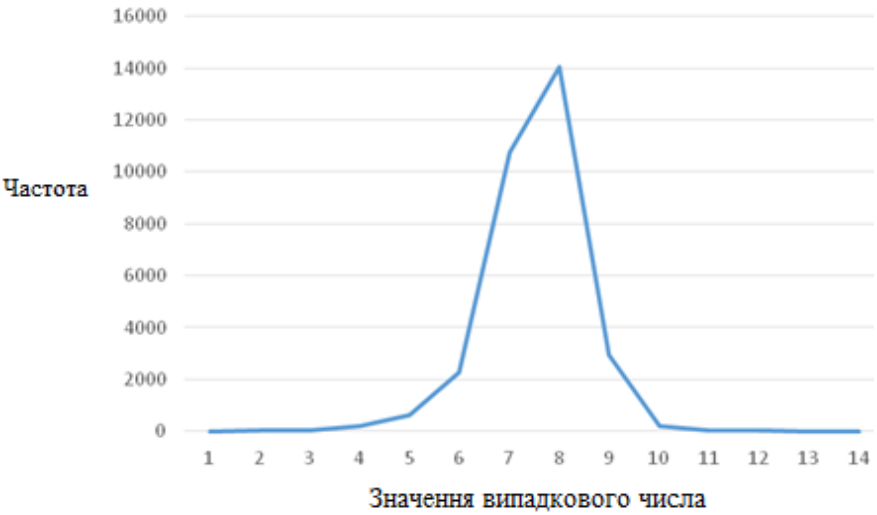

Рис. 1. Розподіл чисел згенерованої послідовності

Список використаних джерел

1. Sajedi H. About random number generator [Electronic resource] : [additional materials for course "Introduction to Programming"] / [Hedieh Sajedi] // [Department of Computer Engineering / Sharif University of Technology]. – [2007-05-02]. – Access mode : http://ce.sharif.edu/courses/85-86/2/ce153d/resources/root/Random%20number%20generator.pdf.

References (translated and transliterated)

1. Sajedi H. About random number generator [Electronic resource] : [additional materials for course "Introduction to Programming"] / [Hedieh Sajedi] // [Department of Computer Engineering / Sharif University of Technology]. – [2007-05-02]. – Access mode : http://ce.sharif.edu/courses/85-86/2/ce153d/resources/root/Random%20number%20generator.pdf.