Методи формування псевдовипадкових чисел для псевдонедетермінованих геш-функцій

Баришев Ю. В.[1], Кравчук Т. А.[2]

[1]К.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет м. Вінниця, Україна, yuriy.baryshev@gmail.com
[2] Студентка, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, kravchuktetiana95@gmail.com

Анотація – Для реалізації концепції псевдонедетермінованого гешування необхідні специфічні методи генерування псевдовипадкових чисел. Досліджено відомі генератори псевдовипадкових чисел та запропоновані нові методи формування послідовностей псевдовипадкових чисел. Розроблена програма, що дозволяє виконувати дослідження статистичних характеристик генераторів. Проведений порівняльний аналіз відомих та нових підходів до генерування псевдовипадкових чисел.

Ключові слова: гешування, конструкція гешування, генератори псевдовипадкових чисел, псевдовипадкові послідовності.

Methods of pseudo-random number generation for pseudonondeterministic hash-functions

Baryshev Y. V. 1, Kravchuk T. A.2

[1] PhD (ukr), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95,, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com;
2Student, Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, kravchuktetiana95@gmail.com

Abstract – Methods of pseudo-random number generation are required to implement the pseudonodeterministic hasing conception. Known pseudo-random number generators were considered and new methods of pseudo-random numbers sequences were presented. The program, which provides the necessary statistics characteristics for the research, was developed. Comparative analysis of known and new approaches to generating pseudo-random numbers was performed.

Keywords: hashing, hash constructions, pseudo-random number generators, pseudo-random number sequences.

Вступ

Для захисту інформаційних ресурсів активно використовуються механізми гешування інформації, зокрема для обчислення контрольної суми з метою перевірки автентичності повідомлень, цифрових підписів, пошуку однакових наборів даних, безпечного зберігання паролів та інших конфіденційних даних в області пам'яті та ін. [1]

Окрім атак, що в основі використовують криптоаналіз, наразі залишається актуальною проблема захисту від загальних атак, які використовують мультиколізії [2].

Можливим способом її розв'язання є розробка нових конструкцій гешування, що мали б підвищену стійкість до цих атак.

Дослідження в даній галузі виявили, що саме ітеративність процесу гешування часто є причиною можливості побудови зловмисником мультиколізій [3].

Відповідно для підвищення стійкості конструкцій гешування пропонується порушувати цю ітеративність. Одним з можливих підходів є псевдонедетерміноване гешування [4].

Для реалізації псевдонедетермінованого гешування необхідні специфічні методи генерування псевдовипадкових чисел, які поміж іншим дозволятимуть генерувати числа у змінних діапазонах значень.

Метою дослідження є підвищення стійкості геш-функцій до загальних атак шляхом дослідження відомих генераторів псевдовипадкових чисел (ГПВЧ) та розробці нових підходів.

Відомі генератори псевдовипадкових чисел

У дослідженні розглядалися такі відомі ГПВЧ: лінійний та квадратичний конгруентні, а також на основі чисел Фібоначчі.

Лінійний конгруентний генератор псевдовипадкових чисел – це генератор з вхідними параметрами (x_0, a, c, M), який утворює послідовність псевдовипадкових чисел за допомогою рекурентного співвідношення:

$$x_{i+1} = (ax_i + c) \bmod N, i = 0,1,...$$

Квадратичний конгруентний генератор описується наступним рекурентним співвідношенням:

$$x_{i+1} = \left(dx_i^2 + ax_i + c\right) \bmod N, i = 0,1,...$$

Далі також наведена рекурентна формула конгруентного генератора, що використовує множення з перенесенням:

$$x_{t+1} = (ax_t + c_t) \bmod N, t = 0,1,...,$$

де $c_t = c(x_{t-1}, x_{t-2}, ..., x_0)$ змінюється на кожній ітерації і водночас залежить від попередніх результатів ітерацій таким чином:

$$c_t = \left[\frac{ax_{t-1} + c_{t-1}}{N} \right].$$

Вигляд рекурентного співвідношення, що описує ГПВЧ за принципом чисел Фібоначчі:

$$x_i = \left(x_{i-r} \Diamond x_{i-s}\right) \bmod N,$$

де $i = r, r+1, r+2, ...,$ для початкових значень $x_0, x_1, ..., x_{r-1}$, де $r, s \in N, (r > s)$ - параметри генератора; $\Diamond$ - деяка бінарної операція [5].

Досліджені методи генерування псевдовипадкових чисел не забезпечують виконання вимог щодо високого ступеня нелінійності у залежності псевдовипадкового числа, отриманого на поточній ітерації, від числа, що було отримане на попередній, або не забезпечують рівномірність розподілу чисел.

Для усунення цього недоліку пропонується розробка та дослідження нових підходів до генерування псевдовипадкових чисел.

Запропоновані методи генерування псевдовипадкових чисел

Розглянуто властивості псевдовипадкових послідовностей, утворених поєднанням принципів квадратичного конгруентного генератора та використання рекурентного приросту:

$$x_{i+1} = \left(dx_i^2 + ax_i + c_i\right) \bmod N, i = 0,1,...;$$

$$c_i = \left[\frac{ax_{i-1} + c_{i-1}}{N} \right].$$

Також приріст розглядався генератор, в якому приріст змінювався таким чином:

$$c_i = \left[\frac{dx_i^2 + ax_i + c_i}{N} \right].$$

Пропонується спосіб удосконалення ГПВЧ на основі чисел Фібоначчі з використанням псевдовипадкового відхилення:

$$x_i = (x_{i-1} \Diamond x_{i-b}) \bmod N,$$

де параметр b вибирається випадково за допомогою ГПВЧ, наприклад:

$$b_i = (b_{i-1} \Diamond h + g) \bmod i.$$

На етапі формування перших значень масиву псевдовипадкових параметрів пропонується використовувати вхідні дані гешування:

$$b_0 = (x_0 \Diamond x_1 + x_2) \bmod i,$$

При виборі параметру *b* необхідно слідкувати, щоб його подальше використання не спричинило вихід за межі масиву елементів x_i .

Пропонується варіант, з двома випадковими відхиленнями:

$$x_i = (x_{i-a} \Diamond x_{i-b}) \bmod N,$$

де *a* і *b* обираються випадково.

Параметри *a* і *b* можуть розраховуватись попередньо описаними способами, а також залежати одне від одного:

$$b_i = (a_{i-1} \Diamond h + g) \bmod i,$$
$$a_i = (b_{i-1} \Diamond h + g) \bmod i.$$

Для вибору значень відхилень пропонується використовувати як відомі ГПВЧ, так і комбіновані, а також будувати прямі та перехресні залежності від попередніх значень відхилень і згенерованих псевдовипадкових чисел.

Замість бінарної операції, позначеної як $\Diamond$, у дослідженнях використовувались операції додавання та множення. Однак можливе використання й інших операцій.

Запропоновано генератор псевдовипадкових чисел з умовою парності, що описується так:

$$x_{i+1} = \left((x_i \Diamond x_{i-1}) * x_i \bmod 2 - i * (x_i \bmod 2 - 1) \Diamond x_i\right) \bmod N$$

Варіації з бінарною операцією, позначеною $\Diamond$, аналогічні попереднім, проте в описаному варіанті

не рекомендовано використання множення через значне порушення рівномірності.

Даний варіант дозволяє згенерувати нелінійну послідовність, проте для досягнення кращих показників рівномірності послідовностей пропонуються різні модифікації ГПВЧ з умовою парності.

З додаванням і-го елемента за формулою:

$$x_{i+1} = \left(\left(x_i \Diamond x_{i-1}\right) * \left(x_i \bmod 2\right) - \left(x_i \bmod 2 - 1\right) \Diamond x_i + i\right) \bmod N$$

Дана модифікація дозволяє забезпечити обов'язкове чергування парності/непарності в межах декількох сусідніх ітерацій.

З додатковим і-тим множником:

$$x_{i+1} = \left(i * \left(\left(x_i \Diamond x_{i-1}\right) * \left(x_i \bmod 2\right) - \left(x_i \bmod 2 - 1\right) \Diamond x_i\right)\right) \bmod N$$

Для перевірки парності можна використовувати не тільки попередній елемент послідовності псевдовипадкових чисел. Умову парності пропонується застосовувати до результату виконання бінарної операції над кількома елементами послідовності:

$$x_{i+1} = \left(\left(x_i \Diamond x_{i-1}\right) \bmod 2\right) * \left(\left(x_i \Diamond x_{i-1}\right) \bmod N\right) - \\ - \left(\left(x_i \Diamond x_{i-1}\right) \bmod 2 - 1\right) * \left(\left(i \Diamond x_i\right) \bmod N\right)$$

або за номером *i* самої ітерації:

$$x_{i+1} = \left(i \bmod 2\right) * \left(\left(x_i \Diamond x_{i-1}\right) \bmod N\right) - \\ - \left(i \bmod 2 - 1\right) * \left(\left(i \Diamond x_i\right) \bmod N\right)$$

Також пропонується вдосконалювати даний метод генерування псевдовипадкових чисел, використовуючи складніші моделі з кількома потоками обчислень та розгалуженням за перевіркою не тільки на парність, а й подільності попереднього елемента послідовності на інші числа.

Найкращі характеристики продемонстрував модифікований лінійний конгруентний генератор, що формалізується так:

$$x_{i+1} = \left(\left(ax_i + c\right) \bmod N_1\right) \bmod N_2,$$

де $N_1 > N_2$.

Варіюючи значення N_2 отримується послідовність чисел, яка розподілена рівномірно. При цьому дана властивість не залежить від значення N_2.

ВИСНОВКИ

У даній роботі представлено дослідження властивостей генераторів псевдовипадкових чисел, що використовуються в деяких конструкціях гешування підвищеної стійкості до загальних атак для реалізації концепції псевдонедетермінованого гешування.

На основі досліджень розроблена програма, результатом роботи якої є статистичні показники, необхідні для оцінки характеристик досліджуваних генераторів псевдовипадкових чисел.

В результаті відзначено, що серед відомих ГПВЧ рівномірність забезпечують лінійний і квадратичний конгруентні, проте послідовності є лінійними. А генератори за принципом чисел Фібоначчі та конгруентний, що використовує множення з перенесенням, породжують досить нерівномірні послідовності псевдовипадкових чисел, проте забезпечують відносно високу нелінійність.

У запропонованих підходах спостерігається вища нелінійність, проте нерівномірність послідовностей для більшості запропонованих варіантів генерування залишається проблемою, для розв'язання якої будуть проводитись подальші дослідження.

Внаслідок проведених досліджень визначено модифікацію лінійного конгруентного генератора, властивості якого дозволили досягти поставленої мети досліджень.

ЛІТЕРАТУРА REFERENCES

[1] Ferguson N. Practical Cryptography– 2nd ed.// Ferguson N., Schneier B. //New York: John Wiley & Sons, Inc., – 2003 – 493с.

[2] Joux A. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions / Antoine Joux// Lecture Notes in Computer Science. – 2004. – № 3152. – С. 306-316.

[3] Лужецький В. А. Конструкції хешування стійкі до мультиколізій / Лужецький В. А., Баришев Ю.В. // Наукові праці ВНТУ. – №1. – 2010. – 8 с.

[4] Лужецький В. А. Концепція псевдонедетермінованого хешування / В. А. Лужецький, Ю. В. Баришев // Системи управління, навігації та зв'язку. – №3, 2010. – С. 94-98.

[5] Харин Ю.С. Математические и компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич// МН: Новое знание – 2003. – 193 с.