Столыпинский вестник

Научная статья

Original article

УДК 51-74

ПРИМЕНЕНИЕ И РЕАЛИЗАЦИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

APPLICATION AND IMPLEMENTATION OF PSEUDORANDOM SEQUENCES

Поляков Е.С., студент 4 курс, факультет «Конструирование и технология электронных средств» Московский Государственный Институт имени Н.Э. Баумана Россия, г. Москва genylego@yandex.ru

Моисеев Р.Р., студент 4 курс, факультет «Конструирование и технология электронных средств» Московский Государственный Институт имени Н.Э. Баумана Россия, г. Москва genylego@yandex.ru

Polyakov E.S., 4th year student, Faculty of Design and Technology of Electronic Means, Bauman Moscow State Institute, Moscow, Russia genylego@yandex.ru

Moiseev R.R., 4th year student, Faculty of "Design and Technology of Electronic Means" Bauman Moscow State Institute Russia, Moscow genylego@yandex.ru

Аннотация. Статья посвящена использованию псевдослучайных последовательностей и генераторов случайных чисел в различных областях, таких как криптография, информационная безопасность, тестирование алгоритмов, сетевые протоколы, математическое моделирование и статистический анализ. В

статье рассматриваются различные методы генерации псевдослучайных чисел, включая линейный конгруэнтный метод, метод Фибоначчи, метод Мерсенна, генерацию на основе хэш-функций и метод Монте-Карло. Также особое внимание уделяется использованию сдвиговых регистров с обратной связью для генерации псевдослучайных последовательностей с высокой степенью случайности и равномерности.

The article is dedicated to the use of pseudo-random sequences and random number generators in various fields, such as cryptography, information security, algorithm testing, network protocols, mathematical modeling, and statistical analysis. The article explores various methods of generating pseudo-random numbers, including the linear congruential method, Fibonacci method, Mersenne method, generation based on hash functions, and the Monte Carlo method. Special attention is also given to the use of feedback shift registers for generating pseudo-random sequences with a high degree of randomness and uniformity.

Ключевые слова: псевдослучайные последовательности, генераторы случайных чисел, информационная безопасность, сетевые протоколы, математическое моделирование, статистический анализ.

Keywords: pseudo-random sequences, random number generators, information security, network protocols, mathematical modeling, statistical analysis.

Псевдослучайная последовательность (ПСП) представляет собой последовательность чисел, которая приближается к случайной. Такие последовательности имеют определенную периодичность, которая известна приемнику и передатчику.

Псевдослучайные последовательности нашли свое применение в следующих областях:

– криптография и защита информации;

Здесь ПСП используются, например, для получения ключевой последовательности используемого алгоритма шифрования, для генерации гаммы поточных шифров, а также для выработки векторов инициализации

(блочных шифров). Случайные последовательности незаменимы при формировании паролей и пользовательских ключей. Кроме этого, они могут использоваться для внесения неопределенности в результаты работы различных алгоритмов защиты информации, а также в длительность выполнения шагов алгоритмов для защиты от утечек по побочным каналам. Они также необходимы при формировании случайных запросов при аутентификации и решении многих других задач.

– проверка алгоритмов;

Важной задачей является проверка правильности работы программ. Тестирование – достаточно долгий и трудоемкий процесс. Для его осуществления требуется большой объем входных данных. Использование генераторов случайных чисел повышает эффективность тестирования и позволяет экономить время.

– сетевые протоколы;

ПСП могут использоваться, например, в качестве сессионных ключей, а также для выработки случайных параметров протокола, что обеспечивает уникальность его различных реализаций.

– математическое и имитационное моделирование;

При моделировании сложных физических, технологических и социально-экономических систем и процессов обойтись без применения источников случайности не представляется возможным.

– математическая статистика;

Математическая статистика изучает приближенные методы сбора и анализа данных по результатам эксперимента для выявления существующих закономерностей, т.е. нахождение законов распределения случайных величин и их числовых характеристик. Необходимой составляющей выборочных методов является формирование представительных выборок из генеральной совокупности с использованием случайных чисел.

Свойства псевдослучайных последовательностей отличаются от свойств случайных последовательностей. Вот некоторые из наиболее важных свойств псевдослучайных последовательностей:

– Случайность

Псевдослучайная последовательность должна выглядеть случайной, то есть ее числа должны быть непредсказуемы, и не должно быть видно никаких закономерностей в последовательности.

– Периодичность

Последовательность должна иметь большой период, то есть она должна быть длинной и не повторяться в течение длительного времени.

– Безопасность

Псевдослучайная последовательность должна быть достаточно безопасной для использования в криптографических целях, то есть не должно быть возможности предсказать следующее число в последовательности на основе предыдущих чисел.

Эти свойства важны для обеспечения надежности и безопасности в различных приложениях, таких как шифрование данных, генерация ключей и моделирование случайных процессов.

Устройство, формирующее псевдослучайную последовательность, называется генератором псевдослучайной последовательности (ГПСП).

Существует множество способов реализации генераторов псевдослучайной последовательности. Вот некоторые из наиболее распространенных:

– Линейный конгруэнтный метод (ЛКМ)

Это один из самых простых и наиболее распространенных методов генерации псевдослучайных чисел. Он основан на простой рекуррентной формуле, которая генерирует последовательность чисел на основе предыдущего числа. Однако, если не выбрать параметры метода правильно, результаты могут быть непредсказуемыми. Формула для генерации

псевдослучайной последовательности в линейном конгруэнтном методе имеет вид:

$$X_{n+1} = (aX_n + c) \bmod m, \quad (1.1.1)$$

где X_n - текущее число в последовательности; X_{n+1}- следующее число в последовательности; a, c, m - параметры метода, которые выбираются заранее.

Параметр m обычно выбирается как большое простое число, которое является модулем операции в формуле. Параметр a выбирается таким образом, чтобы он был взаимно простым с m и чтобы он имел большой период генерации ПСП. Параметр c выбирается таким образом, чтобы он был меньше m и чтобы не было слишком коротких циклов генерации ПСП.

– Метод Фибоначчи

Этот метод также основан на рекуррентной формуле, но вместо использования только одного предыдущего числа используется несколько предыдущих чисел. Это может привести к более равномерно распределенным числам, чем в случае с ЛКМ. Формула для генерации ПСП в методе Фибоначчи имеет следующий вид:

$$X_n = (X_{n-1} + X_{n-2}) \bmod m, \quad (1.1.2)$$

где X_n - текущий элемент последовательности; X_{n-1} и X_{n-2} - предыдущие элементы последовательности; m - модуль операции.

– Метод Марсенна

Этот метод использует более сложную формулу, чем ЛКМ, и имеет более высокий уровень безопасности. Он может генерировать более длинные последовательности псевдослучайных чисел, чем ЛКМ или метод Фибоначчи. Формула для генерации ПСП в методе Мерсенна имеет следующий вид:

$$X_n = X_{n-r} \oplus (X_{n-r} \gg s) \oplus (X_{n-r} \ll t) \quad (1.1.3)$$

где Xn - текущее псевдослучайное число, Xn-r - число, которое находится на расстоянии r от текущего числа; s и t - константы, которые выбираются заранее.

– Генерация на основе хэш-функций

Хэш-функция - это функция, которая преобразует входные данные произвольной длины в выходные данные фиксированной длины. Хэш-функции обычно используются для вычисления контрольной суммы или проверки целостности данных.

Для генерации псевдослучайной последовательности на основе хэш-функций, можно использовать следующий алгоритм:

1) Выбирается начальное значение (зерно) для генерации ПСП.
2) Используя хэш-функцию, преобразуется зерно в первое число в последовательности ПСП.
3) Полученное число используется как новое зерно для генерации следующего числа в последовательности.

Шаги 2-3 повторяются для генерации всех чисел в последовательности.

Чаще всего хэш-функции представляются в виде математических формул или алгоритмов, которые преобразуют входные данные в хэш-значение. Например, простейшая хэш-функция может работать следующим образом: каждый символ входной строки заменяется числом, а затем все числа складываются и умножаются на некоторую константу. Полученный результат и будет хэш-значением.

Примеры более сложных и распространенных хэш-функций включают MD5, SHA-1, SHA-256 и SHA-3. Эти хэш-функции используют различные математические операции, такие как сдвиги, XOR, побитовые операции и др., для преобразования входных данных в фиксированное хэш-значение заданной длины.

– Метод Монте-Карло

Этот метод используется для генерации псевдослучайных чисел в статистических расчетах, например, при моделировании случайных процессов. Он основан на генерации случайных точек в пространстве и вычислении вероятности попадания в определенные области. Метод Монте-Карло может использоваться для генерации псевдослучайных чисел через генерацию случайных точек в заданной области. Формула для генерации псевдослучайных чисел методом Монте-Карло выглядит следующим образом:

$$X = (b - a)r + a \qquad (1.1.4)$$

где X - сгенерированное псевдослучайное число; a и b - границы интервала, в котором генерируются случайные числа; r - случайное число, сгенерированное методом Монте-Карло в интервале [0,1].

Суть метода заключается в генерации случайных точек внутри заданного интервала [a,b] и преобразовании координаты каждой точки в псевдослучайное число. Для этого, сначала генерируется случайное число r в интервале [0,1], затем оно масштабируется на интервал [a,b] с помощью формулы, приведенной выше.

Чем больше точек будет сгенерировано, тем более равномерно будут распределены псевдослучайные числа в заданном интервале [a,b], что позволяет получить хорошее качество генерации случайных чисел методом Монте-Карло.

Некоторые виды генераторов псевдослучайных чисел, используют свойства полей Галуа, чтобы генерировать псевдослучайные последовательности [2].

Одно из основных свойств, которое используется в генераторах ЛРС (линейных регистров сдвига) в полях Галуа, это то, что эти поля являются конечными полями. Это означает, что элементы поля можно представить как целые числа в определенном диапазоне, и что операции сложения и умножения в поле также являются конечными. Это свойство позволяет генератору ЛРС

генерировать последовательности, которые имеют конечную длину и которые могут быть периодическими.

Другое свойство, которое используется в генераторах ЛРС в полях Галуа, это то, что умножение в поле Галуа обычно является некоммутативным. Это означает, что при умножении двух элементов порядок операндов имеет значение. Это свойство позволяет генератору ЛРС создавать последовательности, которые могут быть более случайными, чем последовательности, созданные с помощью коммутативных операций.

Кроме того, в генераторах ЛРС в полях Галуа используется свойство аддитивной и мультипликативной инверсии. Это означает, что для каждого элемента поля Галуа существует обратный элемент по сложению и по умножению.

Наконец, в генераторах ЛРС в полях Галуа используется свойство неприводимых многочленов. Неприводимые многочлены определенного вида, называемые "примитивными многочленами". Примитивный многочлен – это неприводимый многочлен, для которого корень (называемый "примитивным элементом") является порождающим элементом мультипликативной группы поля Галуа. То есть, любой элемент поля Галуа может быть выражен через примитивный элемент возведением в некоторую степень.

Использование примитивных многочленов в генераторах ЛРС позволяет получать максимально длинные последовательности псевдослучайных чисел, поскольку такие многочлены обеспечивают равномерное распределение значений в последовательности и максимальную длину периода. Кроме того, существует эффективный алгоритм, называемый "алгоритмом Берлекэмпа-Мэсси", который позволяет быстро находить примитивные многочлены для заданной длины последовательности.

Для генерации псевдослучайной последовательности в поле Галуа необходимо выбрать некоторый начальный элемент (называемый "зерно") и затем применять к нему некоторую функцию (называемую "генератором"), которая генерирует новый элемент в поле Галуа на каждом шаге.

Генераторы случайных чисел на основе ЛРС состоят из нескольких регистров сдвига и комбинационных элементов (AND, OR, XOR), которые обеспечивают линейную структуру генератора. Каждый регистр сдвига хранит биты текущего состояния генератора, которые соединены комбинационными элементами для получения следующего бита последовательности. Для генерации псевдослучайных чисел используется не весь битовый вектор, хранящийся в регистрах, а только некоторые его биты, которые считаются наиболее случайными. Эти биты выходят на выход генератора в качестве псевдослучайной последовательности.

Для увеличения криптографической стойкости генераторов ЛРС могут использоваться дополнительные элементы, такие как нелинейные функции (S-блоки), перестановки, замены и т.д. Однако, в таких генераторах необходимо учитывать возможные уязвимости, связанные с выбором неправильных параметров и атаками на конкретные реализации.

В целом, генераторы случайных чисел на основе ЛРС обладают низкой стоимостью, быстродействием и простотой реализации, что делает их популярными во многих областях, где требуется генерация псевдослучайных чисел. Однако, для криптографических приложений рекомендуется использовать более сложные алгоритмы, такие как генераторы на основе хэш-функций или блочные шифры, которые обеспечивают высокую надежность шифрования данных.

ПСП может использоваться для формирования активной шумовой помехи.

Активная шумовая помеха - это метод искажения радиосигнала, при котором на частоту целевого сигнала подается искусственно созданная помеха, что затрудняет его распознавание.

В ПЛИС синтезируется цифровой сигнал (ЛЧМ, ФКМ и др.) с заданными в ПУ параметрами, и суммируется с ПСП. После суммирования, сигнал с выхода ПЛИС поступает на ЦАП, где преобразуется в аналоговый сигнал.

Использованные источники:

1. Д.И. Кларк, "Сравнение генераторов псевдослучайных чисел", в IEEE Transactions on Computers, т. C-39, № 12, с. 1436-1445, декабрь 1990 г.
2. Власенко А.В., Дзьобан П.И. Генерация псевдослучайных последовательностей на основе линейного конгруэнтного метода и полиномиального счётчика // Интеллектуальные технологии на транспорте. 2017. №4.
3. Дж.Х. Чао, "О мощности тестирования случайности", в Журнал американского статистического общества, т. 88, № 423, с. 1057-1067, сентябрь 1993 г.
4. Х. Фурукава, "Генератор псевдослучайных чисел на основе счетчика для симуляции Монте-Карло", в Журнал IEEE Nuclear Science, т. 46, № 6, с. 2368-2372, ноябрь 1999 г.
5. Д.В. Чудовский и Г.В. Чудовский, "Генератор псевдослучайных чисел метода среднего квадрата", в Журнал вычислительной математики и математической физики, т. 33, № 2, с. 149-153, февраль 1986 г.
6. У.К. Картер, "Тестирование случайности и псевдослучайности чисел", в Журнал американского статистического общества, т. 78, № 392, с. 852-856, декабрь 1983 г.

Sources used:

1. D.I. Clark, "Comparison of pseudorandom number generators", in IEEE Transactions on Computers, vol. C-39, No. 12, pp. 1436-1445, December 1990.
2. Vlasenko A.V., Dzoban P.I. Generation of pseudorandom sequences based on the linear congruent method and the polynomial counter // Intelligent technologies in transport. 2017. No.4.
3. J.H. Chao, "On the power of randomness testing", in the Journal of the American Statistical Society, vol. 88, No. 423, pp. 1057-1067, September 1993.
4. H. Furukawa, "Counter-based pseudorandom number generator for Monte Carlo simulation", in IEEE Nuclear Science Journal, vol. 46, No. 6, pp. 2368-2372, November 1999.

5. D.V. Chudovsky and G.V. Chudovsky, "Pseudorandom number generator of the mean square method", in The Journal of Computational Mathematics and Mathematical Physics, vol. 33, No. 2, pp. 149-153, February 1986.
6. W.K. Carter, "Testing the randomness and pseudo-randomness of numbers", in The Journal of the American Statistical Society, vol. 78, No. 392, pp. 852-856, December 1983.

Для цитирования: Поляков Е.С., Моисеев Р.Р., ПРИМЕНЕНИЕ И РЕАЛИЗАЦИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ// Научный сетевой журнал «Столыпинский вестник» №1/2024.