УДК 621.398.96

Я.И. Шпитяк, А.Ю. Аметов, А.К. Григоренко, П.А. Задорожный, А.И. Фоменко, Е.С. Козелкова

Государственный университет телекоммуникаций, Киев

ИСТОЧНИКИ И ОПИСАНИЕ СОВРЕМЕННЫХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

В статье рассмотрено и описано принципы построения генератора псевдопоследовательных чисел. Рассмотрены виды построения генераторов псевдопоследовательных чисел. Так же описание источников случайных чисел. Рассматривается роль построения генераторов псевдопоследовательных чисел в криптографии.

Ключевые слова: *генератор, генератор псевдосучайных чисел, случайные числа, Источники случайных чисел, детерминированные генераторы псевдосучайных чисел, криптография, период генератора.*

Вступ

Генератор псевдослучайных чисел (ГПСЧ, англ. Pseudorandom number generator, PRNG) - алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).

Современная информатика широко использует псевдослучайные числа в самых разных приложениях - от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых генераторов псевдослучайных чисел напрямую зависит качество получаемых результатов. Это обстоятельство подчёркивает известный афоризм математика ORNL Роберта Кавью (англ.) русск.: «генерация случайных чисел слишком важна, чтобы оставлять её на волю случая.

Источники случайных чисел

Источники настоящих случайных чисел найти трудно. Физические шумы, такие как детекторы событий ионизирующей радиации, дробовой шум в резисторе или космическое излучение могут быть такими источниками. Однако применяются такие устройства в приложениях сетевой безопасности редко. Сложности также вызывают грубые атаки на подобные устройства.

Криптографические приложения используют для генерации случайных чисел особенные алгоритмы. Эти алгоритмы заранее определены и, следовательно, генерируют последовательность чисел, которая теоретически не может быть статистически случайной. В то же время, если выбрать хороший алгоритм, полученная численная последовательность будет проходить большинство тестов на случайность. Такие числа называют псевдослучайными числами.

Альтернативным решением является создание набора из большого количества случайных чисел и опубликование его в некотором словаре, называемом «одноразовым блокнотом». Тем не менее, и такие наборы обеспечивают очень ограниченный источник чисел по сравнению с тем количеством, которое требуется приложениям сетевой безопасности. Хотя данные наборы действительно обеспечивают статистическую случайность, они недостаточно безопасны, так как злоумышленник может получить копию словаря.

Генератор псевдослучайных чисел включён в состав многих современных процессоров, например RdRand входит в набор инструкций IA-32.

Детерминированные генераторы псевдослучайных чисел

Никакой детерминированный алгоритм не может генерировать полностью случайные числа, он может только аппроксимировать некоторые их свойства. Как сказал Джон фон Нейман, «всякий, кто питает слабость к арифметическим методам получения случайных чисел, грешен вне всяких сомнений».

Любой генератор псевдослучайных чисел с ограниченными ресурсами рано или поздно зацикливается - начинает повторять одну и ту же последовательность чисел. Длина циклов генератора псевдослучайных чисел зависит от самого генератора и составляет около $2^{n/2}$, где n - размер внутреннего состояния в битах, хотя линейные конгруэнтные и LFSR-генераторы обладают максимальными циклами порядка 2n. Если порождаемая последовательность генератора псевдослучайных чисел сходится к слишком коротким циклам, то такой генератор псевдослучайных чисел становится предсказуемым и непригодным для практических приложений.

Большинство простых арифметических генераторов хотя и обладают большой скоростью, но страдают от многих серьёзных недостатков:

Слишком короткий период/периоды.

Последовательные значения не являются независимыми.

Некоторые биты «менее случайны», чем другие.

Неравномерное одномерное распределение.

Обратимость.

В частности, алгоритм RANDU, десятилетиями использовавшийся на мейнфреймах, оказался очень плохим, что вызвало сомнения в достоверности результатов многих исследований, использовавших этот алгоритм.

Наиболее распространены линейный конгруэнтный метод, метод Фибоначчи с запаздываниями, регистр сдвига с линейной обратной связью, регистр сдвига с обобщённой обратной связью.

Из современных генераторов псевдослучайных чисел широкое распространение также получил «вихрь Мерсенна», предложенный в 1997 году Мацумото и Нисимурой. Его достоинствами являются колоссальный период (219937−1), равномерное распределение в 623 измерениях (линейный конгруэнтный метод даёт более или менее равномерное распределение максимум в 5 измерениях), быстрая генерация случайных чисел (в 2-3 раза быстрее, чем стандартные генераторы псевдослучайных чисел, использующие линейный конгруэнтный метод). Однако, существуют алгоритмы, распознающие последовательность, порождаемую вихрем Мерсенна, как неслучайную.

Генератор псевдослучайных чисел с источником энтропии.

Наравне с существующей необходимостью генерировать легко воспроизводимые последовательности случайных чисел, также существует необходимость генерировать совершенно непредсказуемые или попросту абсолютно случайные числа. Такие генераторы называются генераторами случайных чисел (ГСЧ — англ. random number generator, RNG). Так как такие генераторы чаще всего применяются для генерации уникальных симметричных и асимметричных ключей для шифрования, они чаще всего строятся из комбинации криптостойкого генератора псевдослучайных чисел и внешнего источника энтропии (и именно такую комбинацию теперь и принято понимать под генератора случайных чисел).

Почти все крупные производители микрочипов поставляют аппаратные генераторы случайных чисел с различными источниками энтропии, используя различные методы для их очистки от неизбежной предсказуемости. Однако на данный момент скорость сбора случайных чисел всеми существующими микрочипами (несколько тысяч бит в секунду) не соответствует быстродействию современных процессоров.

В современных исследованиях осуществляются попытки использования измерения физических свойств объектов (например, температуры) или даже квантовыхфлуктуаций вакуума в качестве источника энтропии для генератора случайных чисел.

В персональных компьютерах авторы программных генераторы случайных чисел используют гораздо более быстрые источники энтропии, такие, как шум звуковой карты или счётчик тактов процессора. Сбор энтропии являлся наиболее уязвимым местом генератора случайных чисел. Эта проблема до сих пор полностью не разрешена во многих устройствах (например, смарт-картах), которые таким образом остаются уязвимыми. Многие генераторы случайных чисел используют традиционные испытанные, хотя и медленные, методы сбора энтропии вроде измерения реакции пользователя (движение мыши и т. п.), как, например, в PGP и Yarrow[5], или взаимодействия между потоками, как, например, в JavaSecureRandom.

Генератор псевдослучайных чисел в криптографии

Разновидностью генератора псевдослучайных чисел являются ГПСБ (PRBG) — генераторы псевдо-случайных бит, а также различных поточных шифров. Генераторы псевдослучайных чисел, как и поточные шифры, состоят из внутреннего состояния (обычно размером от 16 бит до нескольких мегабайт), функции инициализации внутреннего состояния ключом или зерном (англ. seed), функции обновления внутреннего состояния и функции вывода. Генераторы псевдослучайных чисел подразделяются на простые арифметические, сломанные криптографические и криптостойкие. Их общее предназначение - генерация последовательностей чисел, которые невозможно отличить от случайных вычислительными методами.

Хотя многие криптостойкие генераторы псевдослучайных чисел или поточные шифры предлагают гораздо более «случайные» числа, такие генераторы гораздо медленнее обычных арифметических и могут быть непригодны во всякого рода исследованиях, требующих, чтобы процессор был свободен для более полезных вычислений.

В военных целях и в полевых условиях применяются только засекреченные синхронные криптостойкие генераторы псевдослучайных чисел (поточные шифры), блочные шифры не используются. Примерами известных криптостойких генераторов псевдослучайных чисел являются

ISAAC, RC4, SEAL, Snow, совсем медленный теоретический алгоритм Блюм — Блюма — Шуба, а также счётчики с криптографическими хеш-функциями или криптостойкими блочными шифрами вместо функции вывода.

Аппаратные ГПСЧ

Кроме устаревших, хорошо известных LFSR-генераторов, широко применявшихся в качестве аппаратных генераторов псевдослучайных чисел в XX веке, к сожалению, очень мало известно о современных аппаратных генераторов псевдослучайных чисел (поточных шифрах), так как большинство из них разработано для военных целей и держатся в секрете. Почти все существующие коммерческие аппаратные генераторы псевдослучайных чисел запатентованы или держатся в секрете. Аппаратные генераторы псевдослучайных чисел ограничены строгими требованиями к расходуемой памяти (чаще всего использование памяти запрещено), быстродействию (1-2 такта) и площади (несколько сотен FPGA- или ASIC-ячеек). Из-за таких строгих требований к аппаратным генераторам псевдослучайных чисел очень трудно создать криптостойкий генератор, поэтому до сих пор все известные аппаратные генераторы псевдослучайных чисел были взломаны. Примерами таких генераторов являются Toyocrypt и LILI-128, которые оба являются LFSR-генераторами, и оба были взломаны с помощью алгебраических атак.

Из-за недостатка хороших аппаратных генераторов псевдослучайных чисел производители вынуждены применять имеющиеся под рукой гораздо более медленные, но широко известные блочные шифры (DES, AES) и хеш-функции (SHA-1) в поточных режимах.

Применение генераторов случайных чисел в лотереях

Попытки создать генератор случайных чисел относятся к 3500 году до н. э. и связаны с древнеегипетской настольной игрой Сенет. В Сенете два игрока играют за две стороны. Ходы определяются с помощью 4-х плоских палочек, что и может считаться генератором случайных чисел того времени. Бросают все четыре палочки сразу. Подсчет очков происходит следующим образом: 1 палочка упала белой стороной вверх - 1 очко и дополнительный бросок; 2 - 2 очка; 3 - 3 очка, 4 - 4 и дополнительный бросок. Одна из сторон палочки черная и если все четыре палочки падали черной стороной вверх - это максимальный результат - 5 очков и дополнительный бросок.

Известный генератор случайных чисел ERNIE применялся на протяжении многих лет для определения выигрышных номеров британской лотереи.

Главные требования к генраторам случайных чисел, используемому для проведения розыгрышей:

- Каждое число получено случайно, не имея ничего общего с другими числами в последовательности;
- Каждое число из целого ряда имеет равные шансы на выпадение;
- Каждое число имеет заданную вероятность появления в любой заданной области значений.

Самый распространенный метод генерации случайных чисел называется линейный конгруэнтный метод, но есть ещё и другой - аддитивный конгруэнтный метод. Эти методы генерируют последовательность чисел, удовлетворяющую условию случайности. Основой для использования этих и других методов генерации случайных чисел служит программное обеспечение, бесконечно генерирующее числа, независимо от того находится ли в данное время участник в процессе игры или нет. Благодаря этому исключается возможность того, что игрок сможет самостоятельно определить метод генерации, использующийся в данный момент, и «угадать» выпадающие числа.

Например, по законам США требуется, чтобы генератор случайных чисел в игровых автоматах функционировал все время. Кроме того, этим вопросом занимаются непосредственно сами поставщики программного обеспечения.

В лотерее «ТОП-3» («ВГТЛ 2 «Победа») для определения победителей используется генератор случайных чисел, разработанный ООО «ОКБ САПР» специально для проведения тиражей лотереи. Аппарат формирует непрерывный поток случайных шумов, которые преобразуются в числа. В заданный момент времени из потока выхватываются текущие значения, которые и являются выигрышной комбинацией.

При использовании генераторов случайных чисел для розыгрышей лотерей, необходимо соблюдение следующих требований:

- Тестирование потока чисел на случайность.
- Исключение возможностей вмешательства с целью подтасовки результатов розыгрыша.
- Передача результатов розыгрыша в центр обработки ставок в момент определения выигрышной комбинации с точностью до миллисекунды.
- Возможность резервирования с автоматическим переключением на запасное оборудование в случае неисправности.

Выводы

Случайные числа требуются в криптографии очень часто. Симметричный ключ шифрования должен выбираться случайным образом. При генерации ключей для асимметричной криптосистемы необходимо иметь достаточно большой объем случайных данных. Корректная реализация асимметричных криптоалгоритмов, например RSA, требует добавлять к каждой порции открытого текста несколько случайных байт.

Однако в компьютере, в общем случае, нет хорошего источника случайности, способного выдавать значительные объемы истинно случайных данных. Поэтому в криптографии находят широкое применение генераторы псевдослучайных чисел.

Псевдослучайные данные совсем не то же самое, что истинно случайные. Генератор псевдослучайных чисел использует детерминированный алгоритм и выдает последовательность значений, зависящую от начального значения (seed value), загруженного в генератор. Зная начальное значение, легко повторить последовательность, выдаваемую генератором.

Список літературы

1. *Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайдер. Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 424 с.*
2. *Кнут Д. Искусство программирования, том 2. Получисленные методы / Д. Кнут. – М.: Изд. дом «Вильямс», 2007. – 832 с.*
3. *Соболь И.М. Численные методы Монте-Карло / И.М. Соболь. М.: Наука, 1977. – 327 с.*
4. *Кремер Н.Ш. Теория вероятностей и математическая статистика: учебник для вузов / Н.Ш. Кремер. – М.: Юнити-Дана, 2000. – 543 с.*
5. *http://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D0%BF%D1%81%D0%B5%D0%B2%D0%B4%D0%BE%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB*
6. *Дональд Э. Кнут. Глава 3. Случайные числа // Искусство программирования = The Art of Computer Programming. — 3-е изд. — М.: Вильямс, 2000. — Т. 2. Получисленные алгоритмы. — 832 с. — 7000 экз. — ISBN 5-8459-0081-6 (рус.) ISBN 0-201-89684-2 (англ.)*

Надійшла до редколегії 11.03.2014

Рецензент: д-р техн. наук, проф. Н.И. Кунах, Государственный университет телекоммуникаций, Киев.

ДЖЕРЕЛА Й ОПИС СУЧАСНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Я.І. Шпитяк, А.Ю. Аметов, О.К. Григоренко, П.А. Задорожний, А.І. Фоменко, Е.С. Козелкова

У статті розглянуто та описано принципи побудови генераторів псевдовипадкових чисел. Розглянуто види генераторів псевдовипадкових чисел. Також опис джерел випадкових чисел. Розглядається роль генераторів псевдовипадкових чисел у криптографії.

Ключові слова: *генератор, генератор псевдовипадкових чисел, випадкові числа, джерела випадкових чисел, детермінуєванні генератори псевдовипадкових чисел, криптографія, період генератора.*

SOURCE PRNG. DESCRIPTION OF MODERN PRNG

Y.A. I. Shpityak, A.YU. Ametov, A.K. Grigorenko, P.A. Zadorozhnyy, A.I. Fomenko, E.S. Kozelkova

The article examines and describes the principles of the pseudorandom number generator. Kinds pseudorandom number generator. As well as a description of sources of random numbers. The role pseudorandom number generator in cryptography.

Keywords**:** *generator, pseudorandom number generator, random numbers, random number sources, determines pseudorandom number generator, cryptography, period generator.*