

В.Б. Говоруха, И.В. Петрусенко, Ю.А. Храпач
Академия таможенной службы Украины

МЕТОДЫ ГЕНЕРАЦИИ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Наведено огляд існуючих методів генерації випадкових та псевдовипадкових чисел, які є обов'язковим елементом сучасних криптографічних систем. Особливу увагу приділено методам квантової криптографії.

Приведен обзор существующих методов генерации случайных и псевдослучайных чисел, которые являются обязательным элементом современных криптографических систем. Особое внимание уделено методам квантовой криптографии.

This article provides an overview of the existing methods of generating random and pseudo-random numbers that are must-have modern cryptographic systems. Special attention is paid to the methods of quantum cryptography.

Ключевые слова: случайные числа, криптографія, генератор случайных чисел, линейно-конгруэнтная функция, квантовая криптография.

Вступление. Для создания паролей и ключей необходимо генерировать случайную величину. Качественный механизм генерации случайных чисел – основа любого безопасного приложения. В связи с этим генератор случайных выборок чисел является необходимым элементом оснащения современных систем защиты информации, в частности систем криптографии. Криптография способна защитить данные от атак, помогает обеспечивать секретность и целостность данных, поэтому на разработку генераторов случайных чисел и исследование закономерностей их работы затрачиваются значительные усилия.

Трудности генерации последовательностей чисел, обладающих заданными статистическими закономерностями, носят фундаментальный характер. В этом нетрудно убедиться, рассматривая три известных подхода к данной проблеме.

Известными подходами к генерации случайных чисел являются методики, основанные на использовании линейно-конгруэнтных функций, а также применение устройства, в качестве которого принимается какой-либо квантовый физический процесс.

Основная часть. В докомпьютерную эру были изданы справочные таблицы случайных чисел (правда, без гарантий, что эти массивы чисел действительно удовлетворяют всем «разумным» статистическим тестам на некоррелированность). Не представляет труда сохранить эти данные в памяти ЭВМ, но немедленно возникает вопрос способа использования такого фиксированного файла. А именно, если пытаться считывать этот файл со случайной позиции, то мы получаем «порочный круг», т. е. возвращаемся к необходимости генерации случайного числа. В настоящее время этот подход признан бесперспективным.

Второй и наиболее распространенный метод состоит в применении арифметического алгоритма, дающего псевдослучайные числа, равномерно распределенные на единичном интервале. Как правило, алгоритм основан на отображении множества допустимых чисел $X = \{x_m\}$ в себя по рекуррентной формуле $f(x_m) = x_{m+1} \in X$. Так как процесс начинается с заданного числа x_0 , то такие последовательности являются воспроизводимыми, что важно для отладки машинных программ.

Этот подход прошел ряд этапов в своем развитии. Если поначалу функции $f(x_m)$ выбирались как можно более сложные и трудно понимаемые, то затем пришли к простым функциям, свойства которых достаточно хорошо изучены. Чаще всего применяют линейно-конгруэнтную функцию вида

$$f(x_m) = ax_m + c \pmod{n}, \quad (1)$$

где $a, c \in X$ и $n = 2^t$ для t -разрядных двоичных целых чисел. Доказана теорема [1], что сгенерированная таким образом последовательность обязательно имеет период (его максимальная длина равна n), при этом наименее значимые двоичные разряды числа $x_{m+1} = f(x_m)$ будут отнюдь не случайными. Конгруэнтные последовательности в конце концов образуют цикл, который повторяется бесконечное число раз.

Доказано также, что общим свойством всех алгоритмов генерации псевдослучайных чисел, использующих рекуррентные соотношения, является корреляция между двумя последовательными числами [2]. Отличие между известными реализациями таких датчиков чисел только в степени, в которой этот эффект проявляется. Например, для генератора псевдослучайных чисел из ранее популярного пакета научных программ SSP фирмы IBM, использующего формулу (1) с величинами $a = 2^{16} + 3$ и $c = 0$,

наблюдается крайне высокая корреляция между тремя идущими подряд числами [2]. Этот факт заставляет серьезно сомневаться в достоверности результатов большого числа статистических исследований.

К линейно-конгруэнтным функциям относится известная функция Rand, которая входит в библиотеки многих языков программирования. Такие функции бесполезны для защищенных сред.

Хороший генератор случайных чисел характеризуется тремя свойствами: равномерным распределением генерируемых чисел, непредсказуемостью значений и поддержкой полного цикла. Линейно-конгруэнтные функции обладают только первым свойством.

Самыми известными из атак, основанных на предсказуемости случайных чисел, можно считать атаки на ранние версии браузера Netscape Navigator. Случайные числа, на основании которых генерировались ключи протокола SSL, оказались легко предсказуемыми, что сводило на нет эффективность SSL-шифрования.

В настоящее время развивается такое направление криптографии, как квантовая криптография. Это метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приема информации всегда выполняется физическими средствами, например при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи. Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы — невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой.

Квантовая наука зародилась в 1984 году, когда был разработан первый протокол квантового распределения ключей, названный BB84.

В связи с развитием квантовой криптографии наиболее перспективным подходом к генерации случайных чисел считается третий подход, связанный с использованием стохастического устройства, в качестве которого принимается какой-либо квантовый физический процесс. Доказано, что квантовые процессы порождают массивы чисел, которые нельзя вычислить с помощью машины Тьюринга. Это означает, что не существует алгоритма, который генерировал бы в точности ту же последовательность, что и «квантовый» датчик случайных чисел. В недавно опубликованных математических исследованиях показано, что генераторы случайных чисел, основанные на квантовых процессах, действительно могут выдавать поток случайных чисел [3].

Известны попытки использования закономерностей испускания электронов горячим катодом или излучения лазера. В последнем случае применялся полупроводниковый лазер с короткими и резкими пиками интенсивности. Лазер пропускался через среду с обратной связью с задержкой, т. е. интенсивность излучения на выходе определялась интенсивностью сигнала на входе и состоянием среды, которое зависело от интенсивности на выходе. Ранее исследователям было известно, что интенсивность подобного луча является процессом квазипериодическим, то есть с течением времени он почти повторяется, поэтому напрямую использовать его в качестве генератора случайных чисел нельзя. Для того чтобы избавиться от квазипериодичности, физики действовали следующим образом. Интенсивность луча замерялась примерно 2,5 миллиарда раз в секунду. Результат каждого измерения записывался в строку длиной в 8 бит. Он вычитался из значения предыдущего измерения, а результат усекался. Таким образом, исследователям удалось избавиться от квазипериодичности и добиться генерации случайного потока нулей и единиц со скоростью примерно 12,5 гигабита в секунду.

Один из недостатков подобных датчиков чисел состоит в том, что результаты измерений могут содержать систематическую, т. е. неслучайную ошибку. Как сообщается, после специальной обработки результатов измерения интенсивности лазерного луча удалось добиться генерации случайного потока нулей и единиц с высокой скоростью.

Другое направление исследований основано на использовании принципа неопределенности (индетерминизма) квантовых систем. Согласно квантовой механике, невозможно точно предсказать, как квантовая частица будет себя вести. Поэтому теоретически истинную случайность системе может обеспечить, например, поведение двух связанных элементарных частиц. В работе [4] исследовался датчик случайных чисел, генерирующий двоичные числа на основе измерений квантовых состояний иона иттербия, который может находиться либо на высоком, либо на низком энергетическом уровне. Чтобы проверить истинность случайности, «спутывались» два таких иона и измерялись их энергетические уровни. Если корреляция полученных значений соответствовала так называемому «ограничению Белла» [4], то случайность полагалась подлинной. Сообщается, что в течение месяца таким образом удалось получить 42 действительно случайных двоичных числа.

В рамках работы [5] проверялась так называемая алгоритмическая случайность потока чисел, выдаваемого «квантовым» датчиком Quantis.

Данный тип случайности является одним из самых сильных: он означает, что для любого алгоритма данный поток будет являться случайным. Сравнение полученного массива проводилось с числами, сгенерированными несколькими компьютерными программами, а также строками цифр из записи числа π . Сообщается, что полученные результаты могут служить подтверждением вывода о том, что квантовые процессы дают действительно случайные числа.

Следует отметить, что метод квантовой криптографии обладает рядом недостатков. Суть уязвимости состоит в несовершенстве аппаратной части «криптографического устройства», а не в возможности влиять каким-либо мифическим образом на законы физики.

Известно, что передаваемое при помощи метода квантовой криптографии сообщение кодируется в последовательности фотонов разной поляризации, движущихся по каналу передачи данных. Некий злоумышленник, желая прочесть сообщение, будет вынужден перехватывать фотоны, чтобы выполнить измерение их поляризационного момента. Однако, как гласит принцип неопределенности квантовых систем Гейзенберга, невозможно измерить какой-либо параметр фотона, не исказив неизбежно другой параметр. Это обстоятельство гарантировало надежность метода квантовой криптографии, потому как получатель сообщения получит измененное сообщение, и факт вмешательства будет обнаружен.

Для объяснения сути уязвимости надо пояснить следующее: при отправке закодированного сообщения его автор выбирает ту или иную поляризацию фотонов, причем выбор поляризационного момента случаен. Получатель сообщения использует некое устройство — «детектор» — чтобы считать моменты поляризации фотонов, причем из-за случайности их выбора автором сообщения результаты считывания будут то верными, то ошибочными.

После того как все акты считывания поляризации выполнены, получатель по открытому каналу отправляет автору сообщения информацию о параметрах считывания, не сообщая самих результатов измерения. Автор отвечает получателю, в каких случаях он ошибся, тоже по открытому каналу. Отбросив результаты неправильных измерений, получатель получит данные о последовательности фотонов, закодированных автором, — эта переданная секретная информация носит название первичного ключа. Чтобы обнаружить факт перехвата сообщений, и автор и получатель по открытому каналу сравнивают результаты считывания поляризации фотонов, — в случае их перехвата эти параметры у автора и получателя совпадать не будут.

Во всей этой сложной системе слабым местом является устройство для считывания поляризационных моментов («детектор»), при помощи которого с фотонами работает получатель. Оказывается, что если «насытить» его фотонами до некоего значения, то детектор утратит способность работать с отдельными квантами света и станет работать как классический прибор. Кроме того, экспериментальная реализация квантовой криптографии натолкнулась на ряд технологических трудностей, наиболее важной из которых является сложность генерации строго однофотонных квантовых состояний.

Выводы. Проанализировав существующие методы генерации случайных и псевдослучайных чисел, можно сделать вывод о том, что алгоритмическая случайность потока чисел, выдаваемого «квантовым» датчиком Quantis, является одной из самых сильных. Заметим, что истинно случайный физический процесс, очевидно, принципиально невоспроизводим, поэтому трудно выявить ошибку в компьютерной программе обработки результатов измерений, которая, согласно известной аксиоме программирования, всегда присутствует в коде.

Библиографические ссылки

1. **Кнут Д.** Искусство программирования на ЭВМ / Д. Кнут. // Получисленные алгоритмы. – Т. 2. – М.: Мир, 1977.
2. **Форсайт Дж.** Машинные методы математических вычислений / Дж. Форсайт, М. Малькольм, К. Моулер. – М.: Мир, 1980. – 280 с.
3. **Cristian S. Calude, Michael J. Dinneen, Monica Dumitrescu, Karl Svozil** Experimental Evidence of Quantum Randomness Incomputability
4. <http://www.nature.com/news/2010/100414/full/news.2010.181.html> .
5. <http://www.idquantique.com/true-random-number-generator/quantis-usb-pcie-pci.html> .

Надійшла до редколегії 11.11.2012 р.