АНАЛИЗ ДОСТАТОЧНОЙ ПРОРАБОТАННОСТИ АМЕРИКАНСКОГО СТАНДАРТА DRAFT SP 800-90B

Ставер Е. В.
ИнфоИнКрипт
Минск, Республика Беларусь
E-mail: {mindi1987}@mail.ru

Документ SP 800-90B определяет принципы построения и требования к источникам энтропии, которые являются частью генераторов случайных чисел, а также тесты для проверки источников энтропии. Он был разработан Национальным Институтом Стандартов и Технологий (NIST), в соответствии с Законом о Федеральной национальной информационной безопасности (FISMA, закон 107-347, 2002г.). НИСТ отвечает за разработку Стандартов и Рекомендаций, включая минимальные требования для обеспечения необходимого уровня информационной безопасности для всех видов деятельности, регулируемой законодательно. Данные Стандарты и Рекомендации не должны использоваться в системах, отвечающих за национальную безопасность. Рекомендации были подготовлены к использованию Федеральными ведомствами. Они могут использоваться негосударственными организациями на добровольной основе и не являются объектами авторского права (ссылки на НИСТ приветствуются). Никакая часть данного документа не может трактоваться как противоречащая действующим стандартам..

Введение

Соответственно раз этот материал предназначен для разработчиков, то приводятся рекомендации по проектированию источника энтропии. В первую очередь это касается обеспечения продукта соответствующей документацией. В ней четко должны быть указаны доверительные границы безопасности, которые должны быть постоянными и не должны зависеть от внешних факторов, таких как, например, наблюдение. Сюда также относится описание границ внешних факторов, при которых источник энтропии будет функционировать в соответствии с ожиданиями. Для источника энтропии также необходимо указать внешние условия для его нормального использования, а также доказать, что уровень энтропии не будет меняться при использовании датчика в нормальных условиях. Подробно рассматриваются такие тесты как тесты времени выполнения, т.е. те, которые выполняются непрерывно на цифровых выборках, полученных от источника шума. Использование подобного рода тестов предполагает, что мы работаем с выборкой как с потоком значений. В документе расписаны четкие требования по оценочному тестированию. Американский документ рассматривает такие тесты как, тест на оценку энтропии для равномерно распределенных последовательностей оценивает энтропию на выходе генератора равномерно распределенной величины, базирующийся на подсчете среднестатистического выходного значения, полученного в результате нескольких наблюдений, тест «хи-квадрат» позволила узнать, насколько созданный нами реальный ГСЧ близок к эталону ГСЧ, т.е. удовлетворяет ли он требованию равномерного распределения или нет. ГСЧ должен удовлетворять требованиям равномерного распределения, или p — это вероятность того, что экспериментальное значение χ^2 эксп. будет меньше табулированного (теоретического) χ^2 теор. или равно ему. При длине блока частотно-блочного теста, равной длине всей последовательности частотный блочный тест переходит в частотный побитовый тест.

I. Результат анализа

По критериям теста на оценку энтропии для равномерно распределенных последовательностей датчик calif.bit проходит, т.к. показывает хорошую энтропию, равную 0.9999998971. Датчик bad5.bit по тому же тесту показывает энтропию равную 0.9778620106. По документу DRAFT 800-90b энтропия должна быть приблизительно равна 1. Что и требовалось доказать, датчик bad5.bit тест не прошел. По критериям теста на кси-квадрат в таблице 1 главы 1, приведены теоретические значения «хи-квадрат» (χ^2 теор.), где p — это вероятность того, что экспериментальное значение χ^2 эксп. будет меньше табулированного (теоретического) χ^2теор. или равно ему. Датчик calif.bit проходит, т.к. показывает экспериментальное значение χ^2 равное 0.07 По критериям теста на коллизии, нужно определить интервалы между коллизиями, т.е. когда один и тот же байт (любой из 256 возможных) повторяется в последовательности. Расстояние между двумя такими "повторами интервал коллизий. Датчик calif.bit проходит, т.к. интервал коллизий равен 18.89 и минимальную энтропию 0.99752, близкую к единице. Датчик bad5.bit имеет интервал коллизий равный 6.17 и минимальную энтропию 0.45039. Тестом датчик бракуется. По критериям частотного теста вычисленное в ходе теста значение вероятности p должно быть не меньше 0,01. В противном случае ($p < 0{,}01$), двоичная последовательность не носит истинно случайный характер. Датчик calif.bit проходит, т.к.

имеет в блоке энтропию равную 0.9953290195. Датчик bad5.bit бракуется, т.к. имеет в блоке энтропию равную 0.7650020135. Тест датчик не прошел. Чем меньше p-значение, тем более весомой называется тестовая статистика, и тем больше оснований отклонять нулевую гипотезу. Датчик calif.bit во всех тестах имеет значение p-val, а датчик bad5.bit имеет p-val 0.00 по всем тестам.

II. Доказательство не достаточной проработанности стандарта

tion (SP) 800-90B, Draft. ности вида 111110000011111, 1111111101110000, когда подряд идут много нулей и единиц, все это чередуется и за счет одинакового количества 0 и 1 определим, как последовательности проходят тесты, хотя и не являются истинно случайными. Производим анализ на основании критериев тестов DRAFT 800-90b, а именно тест на оценку энтропии для равномерно распределенных последовательностей, проверка по критерию «хи-квадрат», частотный побитовый тест, частотный блочный тест. Имеем следующие выводы: 1) тест на оценку энтропии для равномерно распределенных последовательностей - базовый тест, отражающий количество 1 и 0 в последовательности, если оно примерно одинаковое - тест пройден, иначе - не пройден. Критерий кси-квадрат в данном тесте базируется на тех же статистических величинах, следовательно, сама форма последовательности никак не учитывается. С точки зрения теста, последовательности 111110000011 и 10101010101010 будут совершенно одинаковыми. 2) тест на коллизии уже является гораздо более точным и отражает статистическое распределение уже не битовой, а байтовой последовательности, то есть подсчет количества встречаемости различных байт относительно друг друга. Данный тест можно считать на порядки точнее первого, так как при неравномерном частотном распределении нулей и единиц в последовательности (например, 11111111100000000001111111111011) тест будет строго не пройден по причине неравномерности распределения количества встречаемости уникальных байт. Не будет пройден он так же и в случае 101010101010101010101. 3) в частотном тесте последовательность разбивается на блоки и оценка энтропии происходит в пределах конкретного блока. Тест не пройден в случаях, т.к. количество 1 и 0 в последовательности, если оно примерно одинаковое - тест пройден, иначе - не пройден. Критерий кси-квадрат в данном тесте базируется на тех же статистических величинах, следовательно, сама форма последовательности никак не учитывается. С точки зрения теста, последовательности 111110000011111 и 10101010101010 будут совершенно одинаковыми.

III. Заключение

Для получения заведомо известных результатов, тесты американского стандарта работают достаточно стабильно и показывают правильный результат. Но, в случаях, описанных в главе 3, пункт 5 нужно с неуверенностью говорить о достаточной проработанности этого американского стандарта. Например, тест на оценку энтропии для равномерно распределенных последовательностей, то критерий кси-квадрат в нем базируется на тех же статистических величинах, следовательно, сама форма последовательности никак не учитывается. С точки зрения теста, последовательности 111110000011111 и 101010101010 будут совершенно одинаковыми. Следует учитывать методы оценки последовательности в тесте, например, если это тест на коллизии - проходят последовательности с одинаковыми байтами. Анализируя такие последовательности, американский стандарт требует дальнейшей доработки и более глубокого изучения с апробацией результатов на конкретных физических датчиках.

IV. Список литературы

1. National Institute of Standards and Technology Special Publication (SP) 800-90B, Draft.
2. Статистические критерии для оценки энтропии / Е.В. Ставер // Журнал научных публикаций аспирантов и докторантов, физ.,мат. – 2012, № 7. – С.111.
3. Требования к физическим датчикам, изложенным в SP 800-90b / Е.В. Ставер // Научная перспектива, техн. – 2012, № 10. – С.77.
4. Тест на оценку энтропии для равномерно распределенных последовательностей, проверка по критерию «хи-квадрат», частотный побитовый тест и частотный блочный тест DRAFT - SP800-90b / Е.В. Ставер // Научный обозреватель, техн. – 2012, № 12. – С.101.
5. Ставер Е. В. Анализ процедур генерации ключей криптографических алгоритмов. Программная реализация теста на оценку энтропии для равномерно распределенных последовательностей Draft SP 800-90b [Текст] / Е. В. Ставер // Молодой ученый. — 2013. — №8.