УДК 681.306

А.А. Кузнецов, Р.В. Королев, Ю.Н. Рябуха

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

В статье рассматриваются генераторы псевдослучайных чисел, получившие широкое практическое применение во многих областях науки и техники. Показан пошаговый процесс тестирования отдельной двоичной последовательности, на основе использования пакета тестов NIST STS, который предназначен для оценки статистической безопасности криптографических генераторов. Исследуется статистическая безопасность наиболее распространенных генераторов псевдослучайных чисел, обосновываются перспективные направления в их развитии.

Ключевые слова: *статистическая безопасность, генератор случайных чисел, тест, криптография.*

Постановка проблемы в общем виде и анализ литературы

Методы формирования последовательностей псевдослучайных чисел (ППСЧ) получили широкое практическое использование во многих областях науки и техники: в криптографических средствах защиты информации для решения задач обеспечения конфиденциальности, целостности, аутентичности и доступности информационных технологий; при формировании больших ансамблей слабокоррелированных дискретных сигналов для обеспечения помехозащищенности, имитостойкости и скрытности систем управления и связи; для обеспечения правильности функционирования компонентов информационной системы, в том числе обеспечения отсутствия недокументированных возможностей, обеспечение неотслеживаемости информационных потоков в системе, защита авторских прав, прав собственников информации и др. [1 – 4]. Для решения перечисленных задач к методам формирования ППСЧ предъявляются жесткие требования, основными из которых являются: высокая стойкость применяемых алгоритмов к восстановлению секретных ключевых данных, параметризирующих работу генератора ППСЧ; высокая скорость формирования ППСЧ, простота практической реализации в программном и аппаратном виде и др.

Целью данной статьи является исследование статистической безопасности наиболее распространенных генераторов ППСЧ, обоснование перспективных направлений в их развитии.

Методика проведения исследований

Одной из основных составляющих оценки эффективности генераторов ППСЧ является оценка их статистической безопасности [5]. Говоря неформально, алгоритм является статистически безопасным, если последовательность, которую он генерирует, по своим свойствам не уступает «случайной» последовательности. Для экспериментальной оценки того, насколько близко криптоалгоритмы аппроксимируют генераторы "случайных" последовательностей, используются статистические тесты. Предложенный в ходе проведения конкурса на новый национальный стандарт США блочного шифрования Американским Национальным Институтом Стандартов и Технологий пакет тестов NIST STS является одним из подходов к решению задачи оценки статистической безопасности криптографических генераторов.

Порядок тестирования отдельной двоичной последовательности S имеет следующий вид [5]:

1. Выдвигается нулевая гипотеза H_0 – предположение о том, что данная двоичная последовательность *S* случайна.

2. По последовательности S рассчитывается статистика теста c(S).

3. С использованием|употреблением| специальной функции и статистики теста рассчитывается значение вероятности $P = f(c(S)),\ P \in [0,1]$.

4. Значение вероятности P сравнивается с уровнем значимости, $\alpha \in [0.001,0.01]$. Если $P \geq \alpha$, то гипотеза H_0 принимается. В противном случае принимается альтернативная гипотеза.

Пакет содержит в себе 16 статистических тестов (табл. 1). Но фактически, в зависимости от входных параметров вычисляется|исчисляющий| 189 значений вероятности P, которые|какие| можно рассматривать как результат работы отдельных тестов.

Таким образом, в результате тестирования двоичной последовательности формируется вектор значений вероятности $P = \{P_1, P_2 ... P_{189}\}$. Анализ составляющих P_i этого вектора позволяет указать на конкретные дефекты случайности тестируемой последовательности.

В соответствии с методикой решение о прохождении статистического тестирования принимается в случае, если выполняются правила:

5. Правило. Прошло тестирование по всем q тестам, ($q=\overline{1,189}$), и если значение коэффициента rj находится внутри доверительного интервала [0.96, 1.00];

6. Правило. Прошло тестирование по всем q тестам, ($q=\overline{1,189}$), и если для всех тестов по критерию χ^2-Пирсона выполняется условие $P(\chi^2) > 0,0001$.

Для проведения исследований статистической безопасности выбраны следующие параметры: длина тестируемой последовательности n = 106 бит; количество тестируемых последовательностей m = 100; уровень значимости α = 0.01; количество тестов q = 189. Таким образом, объем тестируемой выборки составил N = 106 × 100 = 108 бит.

Результаты исследований

При проведении исследований статистической безопасности использовались генераторы ППСЧ, приведенные в таблице 2. Первые семь генераторов реализованы в программном пакете NIST STS. Восьмой генератор – алгоритм симметричного шифрования FIPS 197 в режиме счетчика, описание доступно на электронном ресурсе [7]. Последний генератор впервые описан в работе [8]. Он основан на избыточных кодах, а его безопасность базируется на чрезвычайно высокой сложности решения задачи синдромного декодирования [9]. Для реализации последнего алгоритма разработан программный пакет, в качестве избыточного кода использован код Боуза-Чоудхури-Хоквингема с параметрами (1023, 453, 127).

Результаты статистического тестирования исследуемых генераторов по правилу 1 приведены в табл. 3.

Таблица 1

Набор статистических тестов NIST STS

№ п/п	Статистический тест	Статистика теста
1	Частотный (монобитный тест)	Нормализованная абсолютная сумма значений элементов последовательности
2	Частотный тест (в середине блока)	Мера согласованности наблюдаемого количества единиц теоретически ожидаемому.
3	Проверка накопленных сумм	Максимальное отклонение значений накопленной суммы элементов последовательности от исходной точки отсчета
4	Проверка серий	Общее количество серий на всей длине последовательности
5	Проверка максимальной длины серии в блоке.	Мера согласованности наблюдаемых значений максимальной длины с теоретически ожидаемыми.
6	Проверка ранга двоичной матрицы	Мера согласованности значения наблюдаемых рангов различного порядка с теоретически ожидаемыми.
7	Спектральный анализ на основе дискретного преобразования Фурье	Нормализованная разность количества наблюдаемых частотных компонент с ожидаемыми, превышающими 95% уровень порога.
8	Проверка перекрывающихся шаблонов	Мера согласованности количества наблюдаемых перекрывающихся шаблонов в последовательности с теоретическим значением.
9	Универсальный тест Маурера	Сумма логарифма расстояния между l-битными шаблонами
10	Энтропийный тест	Мера согласованности наблюдаемого значения энтропии источникас теоретически ожидаемым для случайного источника.
11	Проверка случайных отклонений	Мера согласованности наблюдаемого количества визитов при случайном блуждании в заданное состояние в середине цикла с теоретически ожидаемым
12	Проверка случайных отклонений (вариант)	Общее количество визитов при случайном блуждании
13	Последовательный тест	Мера согласованности количества наблюдаемых m-битных шаблонов с теоретически ожидаемым.
14	Проверка сжатия по алгоритму Лемпеля-Зива	Количество в последовательности различных слов
15	Проверка неперекрывающихся шаблонов	Мера согласованности наблюдаемого количества непериодических шаблонов в последовательности с теоретическим значением.
16	Проверка линейной сложности	Мера согласованности наблюдаемого количества событий, которые заключаются в появлении фиксированной длины эквивалентного ЛРР для заданного блока с теоретическим.

Таблица 2

Исследуемые генераторы ППСЧ

№ п/п	Английское название	Русское название
1	G using SHA-1	Генератор на основе алгоритма SHA-1
2	Linear Congruential	Линейный конгруэнтный генератор
3	Micali-Schnorr	Генератор Micali-Schnorr
4	Quadratic Congruential	Квадратичный конгруэнтный генератор
5	G using DES	Генератор на основе алгоритма DES
6	ANSI X9.17 (3-DES)	Генератор на основе алгоритма 3-DES
7	Blum-Blum-Shub	Генератор Blum-Blum-Shub
8	FIPS 197 [6]	Национальный алгоритм шифрования США
9	Pseudo-Random Generator Provably as Secure as Syndrome Decoding (GPSSD) [7]	Генератор ППСЧ, доказуемо безопасный как синдромное декодирование

Таблица 3

Результаты экспериментального тестирования

№ п/п	Генератор	Количество тестов, в которых тестирование прошло M последовательностей (%)		
		M ≥ 99%	M ≥ 96%	M < 96%
1	G using SHA-1	122(65%)	188 (99,5%)	1 (0,5%)
2	Linear Congruential	139 (74%)	189 (100%)	–
3	Micali-Schnorr	130 (69%)	189 (100%)	–
4	Quadratic Congruential	124 (66%)	181 (96%)	8 (4%)
5	G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
6	ANSI X9.17 (3-DES)	121 (64%)	187 (98%)	4 (2%)
7	Blum-Blum-Shub	134 (71%)	189 (100%)	–
8	FIPS 197	126 (67%)	189 (100%)	–
9	GPSSD	144 (76%)	189 (100%)	–

Как видно по представленным в табл. 3 данным, исследуемые генераторы обладают высокими показателями статистической безопасности. Практически все тестируемые последовательности удовлетворяют правилу 1. Исключение составляют последовательности, сформированные генераторами на основе алгоритмов SHA-1, DES, 3-DES и квадратичным конгруэнтным генератором. В тоже время количество не прошедших тестов невелико и не превышает 4 % (для квадратичного конгруэнтного генератора).

Следует отметить высокие показатели статистической безопасности линейного конгруэнтного генератора и генератора Blum-Blum-Shub (рекомендуемого методикой NIST STS для сравнительных исследований). Наивысшие показатели статистической безопасности показал генератор GPSSD - доказуемо безопасный генератор ППСЧ, стойкость которого обосновывается теоретико-сложностной задачей синдромного декодирования.

Таким образом, на основании полученных экспериментальных результатов можно утверждать, что GPSSD является наиболее перспективным по критерию статистической безопасности. Помимо наибольшего количества тестов, прошедших по наиболее жесткому критерию (≥ 99%) данный генератор принадлежит к группе алгоритмов, к которым применимо понятие «доказуемая безопасность» (Provably Security), подробно исследованное в [2]. Практически оно означает, что задача криптоанализа (вычисления секретного ключа) генератора ППСЧ может быть сведена к одной из известных теоретико-сложностных задач, например, факторизации, дискретному логарифмированию и пр. Этот подход позволяет не только статистически, но и теоретически обосновать безопасность применяемого генератора.

Выводы

Проведенные исследования показали, что исследуемые генераторы ППСЧ обладают высокими показателями статистической безопасности. Наибольшую эффективность по данному критерию показал генератор ППСЧ, основанный на использовании избыточных кодов. Данный алгоритм помимо высоких показателей статистической безопасности относится к группе «доказуемо безопасных» генераторов, у которых сложность решения задачи криптоанализа (вычисления секретного ключа) эквивалентна решению хорошо известной теоретико-сложностной задачи (в данном случае задачи синдромного декодирования). Перспективным направлением является исследование циклических свойств ППСЧ, формируемых с использованием GPSSD.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002 – 816 с.

2. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 - Version 0.15 (beta), Springer-Verlag. –, P 829.

3. LandauS. Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard, THE MATHEMATICAL ASSOCIATION OF AMERICA, 111 (February 2004) – P. 89-117.

4. Аунг Т. М. Разработка и исследование стохастических методов защиты программных систем. Автореф. дисс. .. к.т.н.: 05.13.11, 05.13.19 / Московский инженерно-физический институт (государственный университет). – М., 2007. – 20 с.

5. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. Technology Administration U.S. Department of Commerce. – Washington: National Institute of Standards and Technology.-2000. – P 164.

6. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at http://csrc.nist.gov/publications/fips/ fips197/fips-197.pdf

7. Jean-Dernard Fisher, Jacques Stern. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245-255.

8. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

Поступила в редакцию 3.05.2008

Рецензент: д-р тех. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

О.О. Кузнецов, Р.В. Корольов, Ю.М. Рябуха

У статті розглядаються генератори псевдовипадкових чисел, що одержали широке практичне застосування в багатьох областях науки і техніки. Показаний покроковий процес тестування окремої двійкової послідовності, на основі використання пакету тестів NIST STS, який призначений для оцінки статистичної безпеки криптографічних генераторів. Досліджується статистична безпека найбільш поширених генераторів псевдовипадкових чисел, обґрунтовуються перспективні напрями в їх розвитку.

Ключові слова: *статистична безпека, генератор випадкових чисел, тест, криптографія.*

RESEARCH OF STATISTICAL SAFETY OF GENERATORS OF PSEUDO-RANDOM NUMBERS

O.O. Kuznetcov, R.V. Korolov,Yu.M. Rjabuha

The pseudo-random generator, getting the practical wideuse in many regions of scitech, are examined in the article. The incremental process of testing of separate binary sequence is rotined, on the basis of the use of package of tests of NIST STS, which is intended for estimation of statistical safety of cryptographic generators. Statistical safety of the most widespread pseudo-random generators is explored, perspective directions are grounded in their development.

Keywords: *statistical safety, random generator of numbers, test, cryptography.*