Розглянуті реалізації методів оптимізації криптографічних програм за швидкодією, як показують результати тестування, можуть забезпечити синхронізацію процесу шифрування і передачі даних швидкісними каналами зв'язку в комп'ютерних мережах. Зростання об'ємів програм та даних є значними в порівнянні із традиційними методами реалізації алгоритмів ГОСТ 28147-89 [4] і є незначними в порівнянні із зростанням об'ємів системних програм OS Windows.

Література: 1. Михальчук В. М., Ровдо А. А., Рыжиков С. В. Микропроцессоры 80x86, Pentium. Архитектура, функционирование, программирование, оптимизация кода. - М.: "БИТРИКС", 1994. - 398 с. 2. Бердышев Е. Технология ММХ. Новые возможности процессоров P5 и P6. М. "ДИАЛОГ МИФИ", 1998 - 234 с. 3. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М. "Мир", 1979 - 527 с. 4. Мухачев В. А. К вопросу о разработке коммерческих криптосредств, использующих алгоритм ГОСТ 28147. - Праці науково-практичної конференції з питань криптографічного захисту інформації "УкрКрипт - 97", Одеса, 1997.

УДК 681.3.067:681.3.016

ТЕСТИРОВАНИЕ ДВОИЧНЫХ ВЕРОЯТНОСТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МЕТОДОМ БИНОМИАЛЬНОГО ПРЕОБРАЗОВАНИЯ

Тарас Левченко
Научно-технический комплекс "Импульс", г. Киев

Аннотация: **Проведен обзор некоторых методов тестирования двоичных вероятностных последовательностей (ДВП). Отмечены недостатки методов. Предложен метод тестирования, состоящий в анализе функции распределения сумм выборок. Метод проверен на 4 генераторах ДВП. Отмечена чувствительность метода к наличию неслучайной составляющей в ДВП.**

Summary: **The review of some methods of binary probabilistic sequences (BPS) testing is conducted. The lacks of methods are marked. The method of testing based on the analysis of the sampling sums of cumulative distribution function is offered. The method is tested for 4 BPS generators . The test-sensitivity to availability of non-random component in BPS is marked.**

Ключевые слова: **Информационная безопасность, двоичные вероятностные последовательности.**

I Введение

Двоичные вероятностные последовательности (ДВП)

$$\{b_N b_{N-1}..b_1 b_0\}, \tag{1}$$

где

$$b_i = \begin{cases} 1, p_1 = 0.5, \\ 0, p_0 = 0.5, \end{cases} \tag{2}$$

– некоррелированный бит в позиции номер i с дискретной плотностью распределения p, находят широкое применение для кодирования передаваемой информации при защите информационных ресурсов в сетях передачи данных [1]. Для получения ДВП обычно используют математические [2–7] или физические [8] методы генерации последовательностей нулей и единиц. Критерием использования генератора является неповторяемость фрагментов определенной длины при достаточно большом N.

Нечеткость определения понятия неповторяемости ведет к существованию

значительного числа теоретических и эмпирических методов количественной оценки случайности ДВП [9–10]. Как правило, для исследования вероятностных и статистических свойств ДВП следует применять комплекс из нескольких частных тестов, ставящих в соответствие ДВП *r*-мерную интегральную оценку. Мерой соответствия реальных h_k и теоретических p_k оценок случайности ДВП наиболее часто служит критерий хи-квадрат [11] распределения с $r = 1$ степенью свободы

$$\chi = K \sum_{k=1}^{r} \frac{(h_k - p_k)^2}{p}, \tag{3}$$

где K - число независимых наблюдений,
который отвергает теоретические оценки с уровнем значимости α при

$$\chi^2 > \chi^2_{1-a}(r-1),$$

II Постановка задачи

Рассмотрим некоторые [2–7] методы проверки случайности ДВП.

Заполнение «автостоянки».

Из исходной ДВП формируют пары чисел по 7 бит и используют их в качестве координат точек внутри квадрата со стороной 128. Если точка уже занята, накапливается счетчик отсутствия места. Отношение числа успешно поставленных точек к числу попыток оказывается нормально распределенным со средним 3523 и среднеквадратическим отклонением 21,9. Производят не менее 10 проверок.

Подсчет пятибуквенных слов.

Если рассматривать файл исходной ДВП как набор 32-битных слов, выбрать из них 8-битные группы с числом единиц от 0 до 8 и поставить им в соответствие буквы согласно таблице 1, то файл можно преобразовать в последовательность из 5**5 возможных пятибуквенных слов. По каждому слову производится подсчет относительной частоты появления и сравнивается по критерию хи-квадрат с указанным табличным распределением.

Таблица 1

Число единиц	0	1	2	3	4	5	6	7	8
Относительное число групп	0,004	0,031	0,109	0,219	0,273	0,219	0,109	0,031	0,004
Буквенная замена	A	A	A	B	C	D	E	E	E

Проверка потока бит.

$$W_1 = \{b_{20} b_{19} \text{ K } b_1 b_0\}, W_2 = \{b_{21} b_{20} \text{ K } b_2 b_1\}, \text{K }, W_k = \{b_{k+20} b_{k+19} \text{ K } b_k\}$$

Из ДВП (1) формируют последовательность из *k* 20-битовых слов
и определяют количество слов *j*, которых нет в исходном массиве из 2**20 возможных комбинаций. Распределение числа *j* для некоррелированной ДВП является нормальным со средним значением 141,909 и стандартным отклонением 428. Испытание повторяют 20 раз. Аналогичная проверка может проводиться и для других выборок из исходной ДВП.

Проверка ранга двоичной матрицы.

Из ДВП (1) формируют квадратную M*M матрицу

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

$$\begin{pmatrix} b_0 & b_1 & \Lambda & b_{M-1} \\ b_M & b_{M+1} & \Lambda & b_{2M-1} \\ \Lambda & \Lambda & \Lambda & \Lambda \\ b_{MM} & b_{MM+1} & \Lambda & b_{MM+M-1)} \end{pmatrix},$$

для которой затем определяют ранг. Удовлетворительным считается ранг не ниже *M–3*. Таким же методом может проверяться и выборка с заданным интервалом бит из исходной ДВП.

Проверка сумм перекрывающихся бит.

Из ДВП (1) путем последовательного сложения *M* бит с заданным смещением *k* от начала формируется массив сумм

$$S_1 = \sum_1^M b_i, S_2 = \sum_1^M b_{i+1},..., S_k = \sum_1^M b_{i+k-1}.$$

Массив S_k по определению должен иметь нормальное распределение с некоторой матрицей ковариации. После линейного преобразования матрицы ковариации определяют ранг полученной матрицы, который должен быть не ниже *M–2*.

По мнению автора, перечисленные тесты, хотя и дают объективный результат, но являются достаточно громоздкими. Дисперсия статистических оценок оказывается весьма значительной и не уменьшается по мере увеличения объема выборок. Необходимо разработать интегральный тест, который позволяет оценивать случайность ДВП с вероятностью не ниже 0,99 и достаточно чувствительный к внедрению в ДВП периодической составляющей.

III Основная часть

В основу построения предлагаемого автором теста положено известное свойство [11] биномиального распределения с дискретной функцией распределения вероятностей

$$p_k = C_n^k \theta^k (1-\theta)^{n-k}, \tag{4}$$

где C_n^k - биномиальный коэффициент,

равной вероятности того, что сумма *n* случайных величин, принимающих значение 0 или 1 с вероятностями соответственно θ и (1–θ), равна точно *k*.

Если считать ДВП набором из *n* случайных величин с дискретной функцией распределения (2), то очевидно, что случайная величина

$$B_j = \sum_{l=V_j}^{(y_j+V-1)} b_i, \tag{5}$$

где смещение V=const,

является некоррелированной и имеет биномиальное распределение

$$p_k = C_n^k 2^{-2}. \tag{6}$$

Тестированию были подвергнуты ДВП, образованные 4 генераторами:

Таблица 2

Генератор 1	Линейный конгруэнтный генератор *x:=(ax+c)mod q* при *a*=89141, *c*=18837, *q*=65535, *x*0=3, после округления до 0 либо 1.
Генератор 2	Линейный конгруэнтный генератор *x:=(ax+c)mod q* при *a*=31421, *c*=6927, *q*=255, *x0*=6927, после округления до 0 либо 1.
Генератор	Генератор на основе последовательных сдвигов и сложений из Pascal

3	5.5 после округления до 0 либо 1.
Генератор 4	Физический генератор [8] на основе радиоактивного распада.

где $x0$ - стартовое значение.

Параметры теста : V=16, r=17, число усреднений – 20.

В таблице 3 приведены следующие результаты тестирования по каждому генератору:

- Значения хи-квадрат для выборок, полученных:

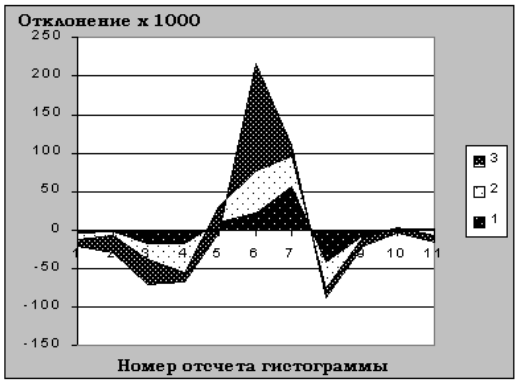
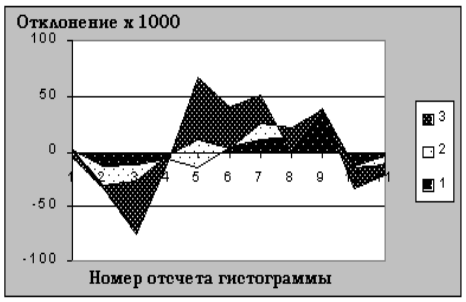
  1 – исходным генератором,

  2 – исходным генератором после введения в каждую выборку 1/8 неслучайной составляющей,

  3 – исходным генератором после введения в каждую выборку 2/8 неслучайной составляющей.

- Графики отклонений гистограмм вариантов 1-3 от теоретического распределения (6).

Таблица 3

№	Z^2	Генератор 1	Z^2	Генератор 2
1	0,68		1,19	
2	2,07		2,48	
3	7,96		6,76	
		Генератор 3		Генератор 4
1	0,87		2,97	
2	1,46		5,16	
3	5,58		9,13	

Неслучайная составляющая вводилась путем задания фиксированных значений бит в определенных позициях. Число таких бит равнялось 2 {1 0} при 1/8 неслучайной составляющей и 4 {1 0 1 0} при 2/8 неслучайной составляющей на выборке из 16 бит.

На рисунках отклонения по 5 отсчетам гистограммы не показаны, поскольку не зависят от величины корреляции.

IV Выводы

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

1. Предложенный подход позволяет уменьшить дисперсию гистограммы случайной величины, что повышает точность статистической оценки функции распределения.

2. Все исследованные генераторы удовлетворяют критерию χ^2, который для уровня значимости $\alpha = 0.99$ и числа степеней свободы 16 равен 5,812 [11].

3. При использовании заданного уровня значимости критерий хи-квадрат оказывается нечувствительным к коррелированности выборок менее 1/4 их длины. Однако его можно использовать для относительных оценок коррелированности ДВП на меньших промежутках, поскольку по мере увеличения коррелированности его значения увеличиваются.

Литература 1. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем.- М.: Горячая линия - Телеком, 2000. - 452 с., ил. 2. Д. Кнут. Искусство программирования для ЭВМ.- Т. 2. - Получисленные алгоритмы. -М.: Мир. - 1977.-482 с. 3. P. L'Ecuyer. Uniform random number generation. // Annals of Operations Research. *-1994.- V. 53. - pp. 77-120. 4. H. Niederreiter. Pseudo-random numbers and optimal coefficients. //* Advances in Mathematics.*-1977.-V. 26. - pp. 99-181. 5. S. K. Park and K. W. Miller. Random number generators: good ones are hard to find. //* Communs of the ACM. *-1988.-V. 31. - pp. 1192-1201. 6. N. S. Altman. Bit-wise behavior of random number generators. //* SIAM Journal of Sci. Stat. Computing.*-1988.-V 9(5) . - pp. 941-949. 7. J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. //* International Statistical Review.-1992.-V. 60. - pp. *167-176. 8. J. Walker. HotBits: Genuine random numbers, generated by radioactive decay. // http://www.fourmilab.ch/hotbits/ 9. J. Eichenauer-Herrmann. Statistical independence of a new class of inversive congruential pseudorandom numbers. //* Math. Comp.-1993.-V. 60. - pp. *375-384. 10. I. J. Good. The serial test for sampling numbers and other tests for randomness. //* Proceedings of Cambridge Philosophical Society.*-1953.-V. 49. - pp. 276-284. 11. Справочник по математике (для научных работников и инженеров). - Г. Корн, Т. Корн. -Изд. 4.-М.: Наука, 1978.- 831 с.*

УДК 681.142.35

ВИКОРИСТАННЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ДЛЯ КРИПТОАНАЛІЗУ АСИМЕТРИЧНИХ СИСТЕМ ШИФРУВАННЯ ЕЛЬ-ГАМАЛА ТА RSA

Микола Карпінський, Ярослав Кінах
Тернопільська академія народного господарства

Анотація: **Розглянуто впровадження ідеї паралелізму для алгоритму решета загального числового поля, що дозволить підбирати надійний ключовий матеріал для асиметричних систем шифрування RSA та Ель-Гамала.**

Summary: **This article deals with the RSA encryption algorithm. Its safety is analysed using the number field sieve method. The algorithm work results allow to define a define a secret key in a simple way.**

Ключові слова: **Паралельні обчислення, метод Гауса, надійність системи шифрування.**

Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Результатом виконання Концепції національної програми інформатизації є: комплект нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високо надійні криптографічні методи захисту інформації тощо.

Найбільш перспективним і динамічним напрямком збільшення швидкості розв'язання прикладних задач є широке впровадження ідей паралелізму в роботу обчислювальних систем. Сьогодні спроектовані і випробувані сотні різноманітних комп'ютерів, що використовують у своїй архітектурі той або інший вид