УДК 004.056.5

МАРКОВСКИЙ А.П.,
ВИНОГРАДОВ Ю.Н.,
ПОВАЖНАЯ Н.С.

К ПРОБЛЕМЕ ОЦЕНКИ КАЧЕСТВА ДВОИЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Статья посвящена проблеме повышения эффективности оценки качества двоичных псевдослучайных последовательностей для защиты информации. Предложен подход к повышению эффективности тестирования псевдослучайных последовательностей. Для определения сложности последовательности с *k*-кратной ошибкой разработана высокопроизводительная технология, использующая нелинейную вос-производящую модель. Показано, что применения разработанной технологии позволяет уменьшить вы-числительную сложность по сравнению с известными методами и, тем самым, сделать возможным тестиро-вание более длинных последовательностей, что обеспечивает повышение надежности оценки их качества.

Paper is dedicated to a problem of increasing of binary pseudorandom sequences for data protection testing efficiency. The approach for increasing the effectiveness of pseudorandom sequences testing for data security system has been proposed. The highly performance techniques for testing of *k*-errors complexity of sequences using nonlinear reproduction model has been developed. It has been shown that implementation of proposed techniques has low calculation complexity in compare to known ones, so it make possible testing of more long sequences and thus ensure highest reliability of testing.

Введение

Генераторы псевдослучайных объектов (чисел, двоичных последовательностей и функ-ций) широко используются в современных информационных технологиях в качестве ключевых элементов систем технической диагностики, статистического и имитационного моделирования, систем мобильной и спутни-ковой связи, при решении математических задач методами Монте-Карло, а также в компьютерных играх и развлечениях.

Важное место занимают псевдослучайные объекты в современных системах защиты информации. Особенно важную роль в этой динамично развивающейся области играют псевдослучайные двоичные последовательнос-ти (ПСДП), которые используются в качестве базового элемента одного из трех типов алгоритмов защиты информации - потоковых алгоритмов[1]. ПСДП широко используются для генерации ключей симметричных алгорит-мов защиты данных и псевдослучайных двоич-ных строк протоколов аутентификации удален-ных пользователей интегрированных систем[1].

В современных условиях роста производи-тельности вычислительных систем и возможностей объединения значительного числа компьютеров в сеть для решения задач наруше-ния защиты, актуальной становится проблема объективной оценки качества ПСДП, ис-пользуемых для защиты информации.

Защитные свойства ПСДП, в теоретическом плане, определяются принципиальной невоз-можностью аналитического решения систем не-линейных булевых уравнений [5]. Именно это свойство булевых преобразований лежит в основе использования двоичных последова-тельностей и булевых функций в системах защиты информации. Исходя из этого наиболее объективным представляется оценка качества указанных средств защиты информации через свойства булевых преобразований, лежащих в их основе.

Таким образом, на современном этапе разви-тия технологии защиты информации актуаль-ной является задача повышения надежности методов оценки качества ПСДП.

Анализ современных методов оценки качества ПСДП

Для эффективного использования ПСДП в современных системах защиты информации они должны удовлетворять определенным критериям. В обобщенном виде можно выделить следующие критерии качества ПСДП:

1. Статистические критерии качества ПСДП, которые включают в себя [6]: оценки распреде-ления, частотность и дисперсию основного и дифференциального распреде-

лений, оценки распределения серий, оценки стационарности статистических генерируемых чисел.

2. Критерий взаимной независимости элемен-тов ПСДП, который оценивается путем анализа двумерного распределения для выявления взаимного влияния элементов последователь-ности, числовых оценок взаимной корреляции, оценки энтропии, а также анализа спектральных характеристик, позволяющего выявить наличие зашумленных периодичностей последователь-ности [6].

3. Возможность экстраполяции последовательности ПСДП путем построения эффектив-ной воспроизводящей модели по заданному фрагменту [1]: формально эта возможность оценивается через параметры модели, вос-производящей заданный фрагмент. Фактически рассматриваемый критерий позволяет оценить с теоретико-информационных позиций возмож-ность предсказания заданного фрагмента по-следовательности.

В ряде работ [1,4] второй и третий критерии качества из приведенного выше перечня рас-сматриваются в качестве одного.

Проведенный анализ использований ПСДП для защиты информации показал, что основным критерием эффективности их применения в этой области является их непредсказуемость, невозможность построения воспроизводящей модели, способной интерполировать заданный фрагмент последовательности.

Формальной оценкой возможности экстра-поляции n-битовой двоичной последователь-ности $S=\{s_1,s_2,\ldots,s_n\}$, $\forall j\in\{1,\ldots,n\}$: $s_j\in\{0,1\}$ выступает сложность воспроизводящей ее модели [1]. В качестве воспроизводящих моделей используется сдвиговый регистр с линейной или нелинейной булевой функцией обратной связи. Соответственно, в первом случае воспроизводящая модель называется линейной, а во втором - нелинейной [1,2].

Установлены критерии [3] оценки возмож-ности экстраполяции последовательностей на основе параметров указанных моделей. Так, при тестировании линейной сложности $L(S)$ n-битовой последовательности S, в качестве критерия невозможности экстраполяции высту-пает равенство $L(S)=n/2$ [1]. Проблема состоит в том, что на практике возможна ситуация, при которой n-битовая последовательность S фор-мально проходит тест на линейную сложность, однако, если инвертировать в S k определенных битов (обозначим модифицированную двоич-ную последовательность через S''), то вполне может оказаться, что $L(S'')<<n/2$, то есть последовательность S'' может быть экстраполирована с использованием воспроизводящей модели $R(S')$. Это означает, что можно экстраполировать и исходную двоичную по-следовательность S с использованием модели $R(S')$ и вероятность битовой ошибки экстра-поляции будет близка к k/n [3].

Задача состоит в нахождении для фиксированного значения k такой локализации единичных компонент вектора $C=\{c_1,c_2,\ldots c_n\}$, $\forall j\in\{1,\ldots,n\}$: $c_j\in\{0,1\}$, $c_1+c_2+\ldots+c_n=k$, для кото-рой значение $L(S\oplus C)$ принимает минимальное значение. Следовательно, это минимальное зна-чение $L(S\oplus C)$ называют линейной сложностью двоичной последовательности S с k-кратной ошибкой (k-error linear complexity of sequence).

Основная проблема практического нахожде-ния линейной сложности последовательности с k-кратной ошибкой состоит в значительной вычислительной сложности решения этой зада-чи. Действительно, для заданной n-битовой двоичной последовательности S вычислитель-ная сложность построения линейной вос-производящей модели при использовании алгоритма Berlekamp-Massey [1] при объеме требуемой памяти $2\cdot n^2$ составляет $O(n^2)$. Следует отметить, что для упомянутого алго-ритма Berlekamp-Massey понятия вычислитель-ной и временной сложности тождественны, поскольку процедура построения линейной воспроизводящей модели в этом алгоритме имеет строго последовательный характер и не может быть распараллелена. Количество q_k возмож-ных вариантов локализации инвертируемых битов последовательности составляет $q_k=n/k$. Если выполняется условие $k<<n$, можно при-ближенно считать, что $q_k \approx n^k$. Следовательно, вычислительная сложность нахождения мини-мального значения $L(S\oplus C)$ составляет $O(n^{k+2})$. Учитывая, что длина последовательности, ко-торая трестируется, составляет 10^5-10^6 бит с перспективой увеличения уже в ближайшие го-ды до 10^8 [4], то очевидной становится пробле-ма практи-

ческой оценки тестирования средств получения случайных и псевдослучайных двоичных последовательностей для защиты информации в компьютерных системах и сетях.

Практика тестирования средств получения случайных и псевдослучайных двоичных последовательностей, ориентированных на ис-пользование в системах защиты информации, показала необходимость профиля изменения сложности последовательности при изменении в ней k бит (введении в нее k-кратной ошибки), где k изменяется от единиц до десятков [4]. Поэтому в последние годы интенсивно раз-вивается концепция построения линейных моделей, которые воспроизводят тестируемую последовательность с k-кратной ошибкой.

В последние годы предложены ряд подходов [4], которые позволяют частично снизить вычислительную сложность рассматриваемой задачи тестирования случайности двоичных последовательностей. Снижение вычислитель-ной сложности, достигается за счет частичного использования при формировании новой линей-ной воспроизводящей модели результатов построения предшествующей модели.

В современных условиях имеет место тенденция увеличения длины двоичной последо-вательности, которая потенциально может быть использована для нарушения системы защиты данных. Это суживает возможности тестиро-вания двоичных последовательностей с ис-пользованием линейной воспроизводящей мо-дели, вычислительная сложность построения которой составляет $O(n^2)$.

Поэтому к настоящему времени задача полу-чения оценки возможности построения при-ближенной воспроизводящей модели ПСДП не решена. Исходя из этого, целью исследований является разработка эффективного способа оценки возможности получения приближенной воспроизводящей модели ПСДП по заданному ее фрагменту.

Использование свойств нелинейной воспроизводящей модели для оценки возможности апароксимации ПСДП с заданной погрешностью

Для расширения возможностей тестирования двоичных последовательностей большой длины было предложено использовать нелинейную воспроизводящую модель[2]. Эта модель спо-собна воспроизвести заданную последователь-ность S и представляет собой m-разрядный сдвиговый регистр, текущие значения разрядов которого образуют вектор $X=\{x_1,x_2,\ldots,x_m\}$, с нелинейной, частично-определенной функцией $f(X)$ обратной связи. Нелинейной сложностью $M(S)$ двоичной n-битовой последовательности S является минимальная длина - m сдвигового регистра с нелинейной функцией обратной связи, который воспроизводит последователь-ность S. В работе [2] теоретически доказано, что последовательность S не может быть экстраполирована, если $M(S)=2\cdot\log_2 n$ и предло-жен алгоритм формирования нелинейной вос-производящей модели. Основное достоинство использования нелинейной воспроизводящей модели для тестирования двоичных последовательностей по сравнению с линейной состоит в том, что ее построение имеет меньшую вы-числительную сложность. Так, вычислительная сложность предложенного в [2] алгоритма по-строения нелинейной воспроизводящей модели составляет $O(n\cdot\log_2 n)$, что существенно меньше вычислительной сложности $O(n^2)$ построения линейной воспроизводящей модели.

В настоящей работе предлагается развитие рассмотренной концепции использования не-линейной воспроизводящей модели для тести-рования случайных и псевдослучайных двоич-ных последовательностей. В частности, предла-гается расширение возможностей нелинейной модели за счет ее применения для определения сложности последовательности S с k-кратной ошибкой.

Анализ возможностей применения нелиней-ной воспроизводящей модели для определения сложности n-битовой двоичной последователь-ности S с k-кратной ошибкой позволяет вы-делить два способа решения этой задачи.

Первый способ позволяет оценить упроще-ние воспроизводящей модели при инверти-ровании k битов последовательности на качест-венном уровне, второй - дает возможность про-извести количественную оценку уменьшения длины сдвигового регистра с нелинейной обратной связью.

Сущность первого способа состоит в оценке полученного значения нелинейной сложности $M(S)$. Предложенный в [2] алгоритм получения нелинейной воспроизводящей модели тестиру-емой двоичной последо-

вательности S заключа-ется в построении бинарного дерева G, описы-вающего частично-определенную нелинейную функцию обратной связи, причем число ярусов этого дерева соответствует значению нелиней-ной сложности $M(S)$. Как показано в [2], математическое ожидание $M(S)$ составляет $2\cdot\log_2 n$. Вполне очевидно, что превышение значения $M(S)$ уровня $2\cdot\log_2 n$ косвенно связано с несба-лансированностью бинарного дерева G. В свою очередь, несбалансированность дерева G свиде-тельствует о возможности уменьшения числа его ярусов за счет его балансирования путем изменения k ребер, что тождественно инверти-рованию k битов тестируемой двоичной после-довательности S. Доказано [2], что значение нелинейной сложности имеет нормальное распределение с математическим ожиданием $2\cdot\log_2 n$ и среднеквадратичным отклонением $0.5\cdot\log_2 n$. Соответственно, вероятность P_1 того, что для полностью случайной последователь-ности S значение нелинейной сложности $M(S)$ превысит $2\cdot\log_2 n$, определяется в виде [2]:

$$P_1 = \frac{\sqrt{2}}{\sqrt{\pi}\cdot\log_2 n}\cdot\int_{2\cdot\log_2 n}^{M(S)} e^{-\frac{(x-2\cdot\log_2 n)^2}{0.5\cdot\log_2^2 n}} \qquad (1)$$

Вычисленное с помощью функции Лапласа значение P_1 сравнивается с пороговым значени-ем $P_П$ и, при условии $P_1 > P_П$, принимается решение о несоответствии тестируемой по-следовательности критерию невозможности экстраполяции с небольшой ошибкой.

Предложенный способ прост в реализации и может быть, модифицирован для линейной воспроизводящей модели. В работе [5] указывает-ся, что "последовательность с большим(относи-тельно уровня $n/2$) значением линейной слож-ности может быть аппроксимирована последовательностью с низким уровнем сложности".

Второй способ не предусматривает перебор всех возможных локализаций модифицируемых битов тестируемой последовательности, а осно-ван на анализе функции обратной связи не-линейной воспроизводящей модели.

Сущность второго способа состоит в вычислении веса Хемминга дифференциала частично определенной булевой функции $f(X)$ обратной связи по каждой из переменных $x_1,\ldots,x_m$. Вычисленный вес Хемминга сравнива-ется с заданным значением k - допустимой кратности ошибки аппроксимации.

Вес Хемминга $HW(\partial f(X)/\partial x_1)$ дифференциала частично определенной булевой функции $f(X)$ по переменной x_1, определяется следующим образом [2]:

$$HW\left(\frac{\partial f(X)}{\partial x_1}\right) = \sum_{x_2,\ldots,x_m\in Z_1} \delta(f(x_1,x_2,\ldots,x_m), f(\overline{x_1},x_2,\ldots,x_m)) \qquad (2)$$

где функция $\delta(y_1,y_2) = y_1\oplus y_2$, если обе булевы переменные y_1,y_2 определены, то есть $\delta(y_1,y_2)=0$ и $y_1,y_2\in\{0,1\}$, если значение хотя бы одной из переменных y_1,y_2 не определено; Z_1 -множество всех 2^{m-1} возможных наборов значений буле-вых переменных $x_2,\ldots,x_m$. Поскольку нелиней-ная модель в виде сдвигового регистра с функцией обратной связи $f(X)$ воспроизводит последовательность S, то фактически значение $q=HW(\partial f(X)/\partial x_1)$ соответствует числу оши-бочных битов при воспроизведении последова-тельности S сдвиговым регистром с функцией обратной связи $f(x_1\oplus 1,x_2,\ldots,x_m)$. Так, значение $q=HW(\partial f(X)/\partial x_1)$ равно числу битов последо-вательности S, которые будут неверно воспро-изведены нелинейной моделью без учета стар-шего разряда сдвигового регистра, то есть с по-мощью $(m\text{-}1)$-разрядного сдвигового регистра.

Из сказанного следует, что если выполняется одно из условий $q=HW(\partial f(X)/\partial x_1)\le k$ или $q=HW(\partial f(X)/\partial x_1)>n-k$, тестируемая двоичная последовательность S может быть аппрокси-мирована последовательностью S' с ошибкой $d=min\{q,n-q\}$ не большей, чем в k битах, причем, нелинейная сложность последовательнос-ти S' на единицу меньше по сравнению с нелинейной сложностью заданной последовательности S: $M(S')=M(S)-1$.

Изложенное иллюстрируется следующим примером. Пусть задана двоичная последовательность $S=\{1,0,1,1,0,0,1,0\}$, в точности совпадающая с последовательностью, приведенной в качестве примера в работе [2]. Нелинейная сложность приведенной последовательности S равна 3-м: $M(S)=3$. Значения частично-определенной нелинейной функции $f(x_1,x_2,x_3)$ обратной связи сдвигового регистра приведены в таблице 1.

Табл. 1. Таблица истинности частично-определенной функции $f(x_1,x_2,x_3)$

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	-
0	0	1	0
0	1	0	-
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	0	-

Значение $q=HW(\partial f(x_1,x_2,x_3)/\partial x_1)=1$. Полу-чим, что заданную последовательность S можно аппроксимировать с одним ошибочным битом последовательностью $S'=\{1,0,1,1,0,1,1,0\}$, не-линейная сложность которой равна 2: $M(S'')=2$. Такое значение нелинейной сложности свиде-тельствует о том, что последовательность S' может быть воспроизведена нелинейной мо-делью в виде 2-разрядного сдвигового регистра и функцией $\varphi(x_2,x_3)$ обратной связи, значения которой представлены в таблице 2.

Важным является определения затрат вычислительных ресурсов, требуемых для реализации предложенного способа тестирования. Вычислительная сложность формирования веса Хемминга дифференциала частично определенной нелинейной булевой функции $f(X)$ от m переменных по переменной x_1 определяется перебором половины таблицы истинности $f(X)$ и составляет $O(2^{m-1})$. Для нелинейной модели $m\approx 2\cdot\log_2 n$ [2], поэтому $O(2^{m-1})=O(2\cdot n)$.

Табл. 2. Таблица истинности частично-определенной функции $\varphi(x_2,x_3)$

x_2	x_3	$\varphi(x_2,x_3)$
0	0	-
0	1	1
1	0	1
1	1	0

Если учитывать вычислительную сложность построения нелинейной воспроизводящей модели - $O(n\cdot\log_2 n)$ [2], результатом которого является формирование таблицы, получаем, что вычислительная сложность определения возможности уменьшения на единицу сложности нелинейной воспроизводящей модели за счет d ошибок аппроксимации заданной двоичной последовательности, составляет $O(n\cdot(\log_2 n+2))$. Это означает, что затраты вычислительных ресурсов на решение указанной задачи незначительно превышают вычислительную сложность построения самой нелинейной воспроизводящей модели.

Полученное значение вычислительной слож-ности существенно меньше по сравнению с использованием для решения аналогичной задачи линейной воспроизводящей модели [4], поскольку в последнем случае затраты вы-числительных ресурсов экспоненционально зависят от кратности k допустимой ошибки аппроксимации - $O(n^k)$. Важно, что значитель-ное уменьшение вычислительной сложности для определения возможности упрощения воспроизводящей модели за счет некоторого количества ошибок аппроксимации заданной двоичной последовательности достигается за счет следующих трех факторов:

- Использование нелинейной воспроизводя-щей модели, размерность $2\cdot\log_2 n$ которой существенно меньше размерности $n/2$ линейной модели.

- Применение предложенного подхода сопряжено с существенно большими объемами требуемой памяти по сравнению с методами [4,5], основанными на использовании линейной модели. Это объясняется тем, что при использо-вании нелинейной воспроизводящей модели формируемая нелинейная функция хранится в виде таблицы истинности, а при линейной вос-производящей модели функция обратной связи формируется в алгебраической форме, требую-щей намного меньшего объема памяти. Также, табличное представление функции обратной связи позволяет ускорить операции, связанные с вычислением ошибки аппроксимации. Вместе с тем, повышенный объем требуемой памяти не выходит за рамки возможностей практической реализации. Так, данный способ оценки воз-можности аппроксимации требует памяти, объем которой составляет $2\cdot 2^m = 8\cdot n$ бит. Для типовой длины тестируемой последователь-ности 10^6 бит, требуемый объем памяти - около одного мегабайта, что вполне реализуемо современными техническими средствами.

- В данном способе задача тестирования су-жена: в разработках [4,5] определяется мини-мальная сложность воспроизводящей модели при всех возможных k-битовых ошибках ап-проксимации. Предложенное решение позволя-ет выявить возможность

уменьшения сложнос-ти воспроизводящей модели при всех возмож-ных k-битовых ошибках аппроксимации. На практике тестирования двоичных случайных и псевдослучайных последовательностей определение такой возможности вполне может быть приемлемым результатом [3].

Для определения минимальной сложности нелинейной воспроизводящей модели при всех возможных k-битовых ошибках аппроксимации заданной последовательности, предложенная процедура может быть применена рекурсивно.

Пусть задана последовательность S длиной n бит и кратность допустимых ошибок аппрокси-мации S нелинейной воспроизводящей моделью с минимальной длиной сдвигового регистра составляет k битов. Надо определить минимать-ную длину сдвигового регистра с нелинейной функцией обратной связи, способного вос-произвести последовательность S с ошибками не более чем в k битах.

Рекурсивное применение предложенной про-цедуры осуществляется в следующем порядке:

1. Для заданной двоичной последовательности S строится нелинейная воспроизводящая модель и частично определенная функция $f(X)$ обратной связи, количество m аргументов кото-рой определяет нелинейную сложность $M(S)$ последовательности S.

2. Для функции по формуле (2) вычисляется Хеммингов вес ее дифференциала по перемен-ной, которая соответствует старшему разряду сдвигового регистра: $q=HW(\partial f(x_1,...,x_m)/\partial x_1)$. Вычисляется значение $d=min\{q,n-q\}$.

3. Если $d \le k$, то в последовательности S инвертируются биты, которые обуславливают зависимость функции f(X) от переменной x_1. Значение уменьшается на величину d: $k:=k-d$. Если k>0, то возврат на пп.1, в ином случае $M(S):=M(S)-1$.

4. Если $M(S) < 1.5\cdot\log_2 n$, то проведенное тестирование двоичной последовательности свидетельствует о нецелесообразности приме-нения генератора, с использованием которого получена последовательность, в системах защи-ты информации.

Вычислительная сложность реализации при-веденной рекурсивной процедуры определяет-ся количеством h шагов рекурсии и составляет $O(h\cdot(n+2)\cdot\log_2 n)$. Это значительно меньше по сравнению с вычислительной сложностью $O(n^{k+2})$ решения рассматриваемой задачи с ис-пользованием известных способов, основанных на линейной воспроизводящей модели.

Выводы

В результате проведенных исследований предложен способ тестирования генераторов случайных и псевдослучайных двоичных последовательностей, ориентированных для использования в системах защиты информации. Способ позволяет оценивать возможность экстраполяции двоичных последовательностей с использованием нелинейной воспроизводя-щей модели, а также, за счет меньшей по сравнению с известными методами вычисли-тельной сложности, обеспечивать возможность существенно увеличить длину тестируемой последовательности и, тем самым, позволяет повысить достоверность оценки пригодности генератора случайных или псевдослучайных последовательностей для систем защиты ин-формации.

Так, тестирование возможности аппроксимации последовательностей длиной 10^8 бит известными методами сопряжено со значительными техническими трудностями [3], в то время как экспериментально доказано, что тестирование таких последовательностей с использованием предложенного способа осуществляется достаточно просто. Обеспечи-ваемая предложенным способом возможность тестирования длинных последовательностей позволяет существенно повысить достовер-ность оценки качества генераторов случайных и псевдослучайных двоичных последователь-ностей применительно к их использованию в системах защиты информации. Достигаемое использованием разработанного способа увеличе-ние оперативности тестирования потенциально позволяет повысить качество проектирования средств генерации случайных и псевдослучай-ных последовательностей.

Список литературы

1. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ.- 2003 – 260 с.

2. Марковский А.П., Мустафа Акрам Ареф Найеф, Бойко А.В. Об одном подходе к определению сложности случайных и псевдослучайных двоичных последовательностей // Вісник національного технічного університету України ”КПІ”. Інформатика, управління та обчислювальна техніка. – 2002.- №37.- С.120-129.
3. Самофалов К.Г., Марковський О.П., Абабне О.А. Оцінка якості генераторів двійкових послідовностей з використанням нелінійної відтворюючої моделі // Проблеми інформатизації та управління. Збірник наукових праць: Випуск 1(19).-К.,НАУ.- 2007.- С.142-147.
4. Чугунков И.В. Система оценки качества генераторов псевдослучайных кодов. // Научная секция МИФИ-2000.- Т.11,12.- С.45-46.
5. Gutierrez J., Shparlinski I.,A., Winterhof A. On the Linear and Nonlinear Complexity Profile on Nonlinear Pseudorandom Number Generators // IEEE Trans. Information Theory.-2003.- Vol. 49.- № 1. – P.60-64.
6. Kurosava K., Sato F., Sakata T., Kishimoto W. A relationship between linear complexity and k-error linear complexity. // IEEE Trans. Information Theory, 2000.- V.46,-№3.-P.694-698.
7. Meidl W., Niederreiter H. On the expected value of the linear complexity and the k-error linear complexity of periodic sequences // IEEE Transaction of Information Theory.- 2002.- Vol. 48.- № 11. - P.2817-2825.
8. NIST Special Publicaion 800-22: A Statistical Test Suite for Random and Pseudorandom Number. 2000. -348 p.