УДК 004.056.55

М.В. ЕСИНА, С.Г. РАССОМАХИН

Харьковский национальный университет им. В.Н. Каразина, Украина

ПСЕВДОСЛУЧАЙНОЕ КОДИРОВАНИЕ ПО МЕТОДУ ЛИНЕЙНОЙ КОНГРУЭНТНОЙ ГЕНЕРАЦИИ

Рассматриваются свойства линейного конгруэнтного генератора и правила построения кодовых слов псевдослучайного кода. Проводится оценка характеристик псевдослучайного кода, получаемого при помощи алгоритма линейного конгруэнтного генератора. Проводится сравнение псевдослучайного кода и равномерно случайного кода по заданным характеристикам. Исследуется зависимость вероятности декодирования с ошибкой от основного параметра – длины блока кода. Исследование проводится методом имитационного моделирования для гауссового канала при одинаковом отношении сигнал/шум. Приводятся иллюстрации результатов имитационного моделирования псевдослучайного кода и равномерно случайного кода. По результатам имитационного моделирования делается вывод, что псевдослучайный код, построенный по алгоритму линейного конгруэнтного генератора, не уступает равномерно случайному коду.

Ключевые слова: *кодовое слово, линейный конгруэнтный генератор, порождающее число, псевдослучайное кодирование, спектр взаимных расстояний.*

Введение

Методы псевдослучайного кодирования представляют одно из новых направлений реализации кодов корректирующих ошибки. На практике для генерации случайных чисел кода, как правило, используется детерминированный алгоритм. Этот алгоритм должен удовлетворять следующим требованиям:

– обладать простотой и, как следствие, быстродействием;

– обеспечивать равномерное распределение чисел в заданном диапазоне;

– иметь максимальный период генерируемой псевдослучайной последовательности чисел;

– не обладать криптографическими свойствами.

Последнее требование предъявляется для обеспечения простоты алгоритма декодирования с той целью, чтобы любое кодовое слово могло быть однозначно идентифицировано по минимальному количеству символов.

Построение псевдослучайного кода с применением линейного конгруэнтного генератора

Традиционно наиболее общий случай задачи канального кодирования, при котором символы сообщений источника S с мощностью алфавита q_s, объединенные в блоки длиной k, отображаются в символы сообщений канала C с аналогичными параметрами $q_c \neq q_s$, $n \neq k$:

$$S(q_s, k) \Leftrightarrow C(q_c, n). \qquad (1)$$

Для обеспечения взаимно однозначного отображения необходимо, по крайней мере, чтобы $q_s^{\,k} = q_c^{\,n}$.

Среди множества детерминированных методов генерации равномерно распределенных в заданном диапазоне чисел наиболее простым, удовлетворяющим перечисленным требованиям, является метод линейного конгруэнтного генератора (ЛКГ) [1]. При его реализации кодовое слово ПСК со скоростью R представляется точкой (вектором) n-мерного пространства: $\vec{X} = \{x_0, \ldots, x_{n-1}\}$.

Скорость R теоретически может быть любой неотрицательной величиной. В соответствии со свойствами ЛКГ, значения элементов $\vec{X}$ определяются правилами [2]:

– $x_0 \in \left[0 \ldots \left(q_s^{\,k} - 1\right)\right]$ – порождающее число (порядковый номер) кодового слова ПСК;

– $x_i = \mathrm{mod}\left[a \cdot x_{i-1} + b, m\right]$, $i \in 1, \ldots, (n-1)$ – числа слова ПСК, порождаемые x_0 по алгоритму ЛКГ;

– a, b, m – целые положительные константы, удовлетворяющие условиям: $m \geq q_s^{\,k}$, b и m – взаимно простые числа, величина $(a-1)$ кратна любому простому числу, которое меньше m и является его делителем;

– величина $(a-1)$ кратна 4, если m кратно 4.

Произвольное i-ое число ПСК связано с порождающим числом x_0 следующей зависимостью:

© М.В. Есина, С.Г. Рассомахин

$$x_i = \mathrm{mod}\left[a^i x_0 + \frac{a^i - 1}{a - 1} b, m\right], \quad i \in 1,\ldots,(n-1). \quad (2)$$

Если известно порождающее число x_0, то остальные числа однозначно определяются из (2) (процесс кодирования). При соблюдении указанных правил генерации чисел достигается взаимно однозначное отображение (1), поскольку период ЛКГ принимает максимальное значение, равное m. При этом следует наложить условие, чтобы

$$m \geq M = 2^k, \quad (3)$$

в противном случае не удастся обеспечить выполнение требования взаимно однозначного соответствия (1). В случае обеспечения (3) с равенством, при кодировании комбинация из k двоичных символов источника может трактоваться как порождающее число x_0 соответствующего кодового слова в алгоритме ЛКГ. При этом получаемый псевдослучайный код является полным в том смысле, что все возможные последовательности используются для представления кодовых слов. Полные ПСК более технологичны для использования не переборных методов декодирования.

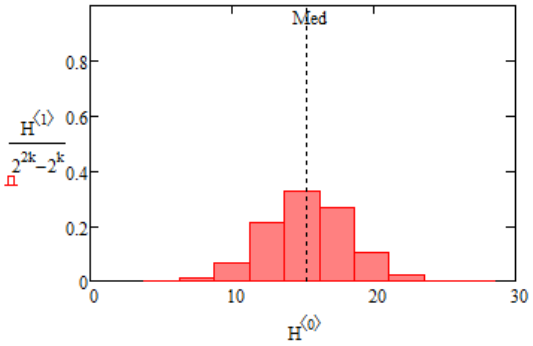
Алгоритм ЛКГ не обладает криптографической стойкостью [1] и, в отсутствии помех, кодовое слово кода однозначно идентифицируется по любому числу из блока длиной n. В данном случае это свойство весьма полезно, так как позволяет при наличии искажений в кодовом слове реализовать квазиоптимальный, легко реализуемый метод декодирования с исправлением ошибок.

Представляет интерес оценка характеристик ПСК, получаемого при помощи алгоритма ЛКГ. Такими характеристиками могут быть минимальное расстояние между кодовыми точками, а также спектр взаимных расстояний кода.

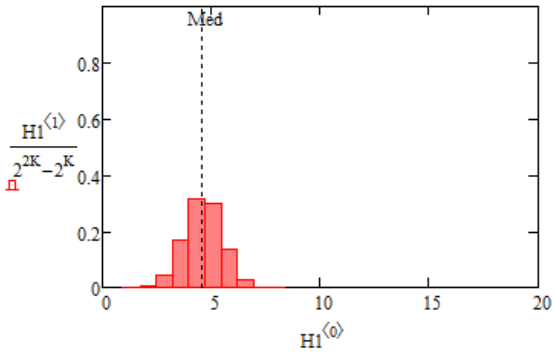
На рис. 1 представлены результаты сравнительного анализа спектров взаимных расстояний равномерно случайного кода (б) и кода, синтезированного в соответствии с правилами ЛКГ (1), (2) (а). Сравнение проведено в одинаковых условиях для небольших значений длин блока.

Как видно из приведенных рисунков, по характеристикам спектра взаимных расстояний ПСК ЛКГ не уступает равномерно случайному коду. Это даёт возможность сделать вывод о правильности выбранного детерминированного алгоритма формирования кодовых книг.

Дополнительным подтверждением справедливости полученных выводов является исследование зависимости вероятности декодирования с ошибкой от основного параметра – длины блока кода. Результаты этого исследования при одинаковом отношении сигнал/шум, выполненные методом имитационного моделирования для гауссового канала представлены на рис. 2.

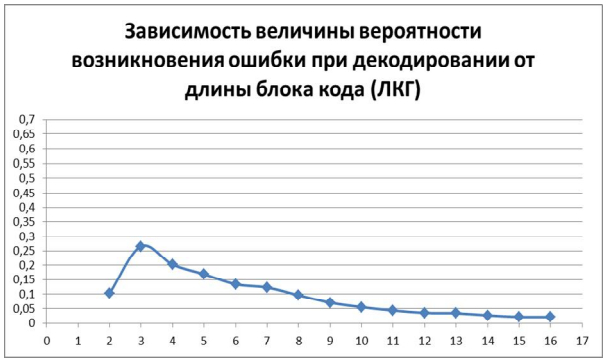


а

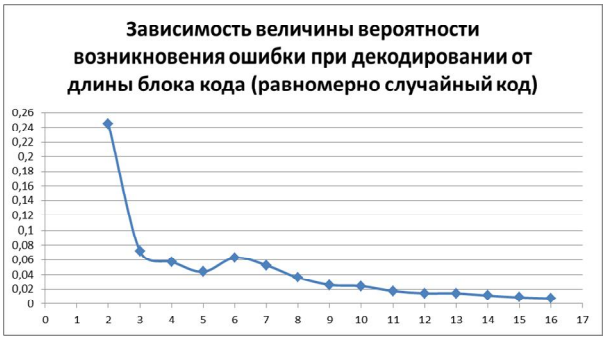


б

Рис. 1. Спектры взаимных расстояний:
а – ПСК ЛКГ; б – равномерно случайный код



а



б

Рис. 2. Графики зависимости величины вероятности возникновения ошибки при декодировании от длины блока кода:
а – при использовании ЛКГ; б – при использовании равномерного распределения

Заключение

Сравнение зависимостей доказывает вполне обоснованную возможность использования простейших детерминированных алгоритмов генерации случайных чисел для получения кодов, близких к оптимальным.

Литература

1. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М.А. Иванов, И.В. Чугунков – М.: КУДИЦ-ОБРАЗ, 2003. – 238 с.

2. Линейные конгруэнтные генераторы [Электронный ресурс]. – Режим доступа: http://r3al.ru/kripto_3/linejnye_kongruentnye_generatory.htm. – 20.01.2013 г.

Поступила в редакцию 1.02.2013, рассмотрена на редколлегии 6.03.2013

Рецензент: д-р техн. наук, проф., проф. каф. инженерии программного обеспечения И.В. Шостак, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

ПСЕВДОВИПАДКОВЕ КОДУВАННЯ ЗА МЕТОДОМ ЛІНІЙНОЇ КОНГРУЕНТНОЇ ГЕНЕРАЦІЇ

М.В. Єсіна, С.Г. Рассомахін

Розглядаються властивості лінійного конгруентного генератора та правила побудови кодових слів псевдовипадкового коду. Проводиться оцінка характеристик псевдовипадкового коду, який отримується за допомогою алгоритму лінійного конгруентного генератора. Проводиться порівняння псевдовипадкового коду та рівномірно випадкового коду за заданими характеристиками. Досліджується залежність ймовірності декодування з помилкою від основного параметру – довжини блока коду. Дослідження проводиться методом імітаційного моделювання для гауссового каналу при однаковому співвідношенню сигнал/шум. Наводяться ілюстрації результатів імітаційного моделювання псевдовипадкового коду та рівномірно випадкового коду. За результатами імітаційного моделювання робиться висновок, що псевдовипадковий код, що побудовано по алгоритму лінійного конгруентного генератора, не програє рівномірно випадковому коду.

Ключові слова: кодове слово, лінійний конгруентний генератор, породжуюче число, псевдовипадкове кодування, спектр взаємних відстаней.

PSEUDO-RANDOM CODING BY LINEAR CONGRUENT GENERATION METHOD

M.V. Yesina, S.G. Rassomakhin

The properties of the linear congruential generator and the rules for constructing a pseudo-random code's words are considered. An estimate of the characteristics of pseudo-random code generated through the algorithm linear congruential generator is conducted. A comparison of the pseudo-random code, and uniformly random code on specified characteristics are conducted. The dependence of the probability of decoding error of the basic parameter – the length of the block of code is investigated. Investigation is conducted by simulation for Gaussian channel with the same signal/noise ratio. An illustration of results of simulation pseudo-random code and uniformly random code are given. According to the simulation results it is concluded that the pseudo-random code constructed by the algorithm of the linear congruential generator, does not yield a uniformly random code.

Key words: code word, linear congruential generator, generating a number, pseudo-random coding, spectrum of mutual distances.

Есина Марина Витальевна – студентка факультета компьютерных наук, каф. безопасности информационных систем и технологий, Харьковский национальный университет им. В.Н. Каразина, Харьков, Украина, e-mail: rinayes20@gmail.com.

Рассомахин Сергей Геннадиевич – д.т.н., доцент каф. безопасности информационных систем и технологий, Харьковский национальный университет им. В.Н. Каразина, Харьков, Украина.