МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОМУНИКАЦИЙ

Международная научно-техническая конференция

СОВРЕМЕННЫЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Материалы научно-технической конференции

Том III
Развитее информационных технологий

17– 20 ноября 2015 г.

Киев

УДК 004.056

В сборнике обобщены материалы конференции, которая проходила на базе Государственного университета телекоммуникаций в период с 17.11.2015 по 20.11.2015 года. В материалах освещаются актуальные вопросы создания и внедрения современной информационной инфраструктуры, как основы построения современного информационного общества.

Сборник рассчитан на преподавателей, аспирантов, студентов, руководителей государственных органов, предприятий и организаций, которые принимают решения в области информационных технологий.

У збірнику узагальнені матеріали конференції, яка проходила на базі Державного університету телекомунікацій в період з 17.11.2015 по 20.11.2015 роки. В матеріалах висвітлюються актуальні питання створення і впровадження сучасної інформаційної інфраструктури, як основи побудови сучасного інформаційного суспільства.

Збірник розрахований на викладачів, аспірантів, студентів, керівників державних органів, підприємств та організацій, які приймають рішення в галузі інформаційних технологій.

This guide is the comprehensive assembly of the Materials from the Conference, which was helded at the State University of Telecommunications in the period from 11.17.2015 to 11.20.2015. These articles describe urgent issues of creation and implementation of modern information infrastructure as the basis for building a modern informational society.

The inforamation is intended for the teachers, postgraduates, students, heads of state bodies, enterprises and organizations who make decisions in the field of information technology.

Все тексты представлены в оригинальном авторском вари анте.
Напечатано в редакционно-издательском центре.

СОДЕРЖАНИЕ

***Штомпель Н.А.**, к.т.н., доцент,*
Украинский государственный университет железнодорожного транспорта,
г. Киев, Украиына

ПОСТРОЕНИЕ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ НА ОСНОВЕ ПРИРОДНЫХ ВЫЧИСЛЕНИЙ

Рассмотрены способы математического описания и особенности кодов с малой плотностью проверок на четность. Сформулирована задача построения нерегулярных кодов с малой плотностью проверок на четность для различных моделей каналов связи. Предложен подход к решению данной оптимизационной задачи на основе процедур природных вычислений.

The methods of mathematical description and features of low density parity check codes are considered. The problem of constructing irregular low density parity check codes for different models of communication channels are formulated. An approach to solving of this optimization problem based on procedures of natural computing are proposed.

Для повышения достоверности передачи информации в современных телекоммуникационных системах широко применяются коды с малой плотностью проверок на четность, которые характеризуются разреженной проверочной матрицей определенной структуры [1, с. 21 – 26]. Данные коды обладают высокой эффективностью вблизи пропускной способности канала связи и меньшей вычислительной сложностью методов декодирования по сравнению с турбо-кодами.

Характеристики кодов с малой плотностью проверок на четность определяются видом графа Таннера, матрица инцидентности которого соответствует проверочной матрице. При этом распределение ненулевых символов в проверочной матрице данных кодов зависит от порядка соединения символьных и проверочных вершин графа Таннера. В зависимости от структуры графа Таннера и соответствующей проверочной матрицы выделяют регулярные и нерегулярные коды с малой плотностью проверок на четность, при этом последние обладают лучшими характеристиками при использовании методов итеративного декодирования. Таким образом, актуальной задачей является построение нерегулярных кодов с малой плотностью проверок на четность с заданными характеристиками с учетом особенностей различных моделей каналов связи.

Показано, что данная задача состоит в поиске распределений степеней символьных и проверочных вершин графа Таннера, которые обеспечивают наименьшее значение вероятности ошибки декодирования для некоторой модели канала связи. Для формализации задачи построения нерегулярных кодов с малой плотностью проверок на четность предложена соответствующая целевая функция и определена область допустимых решений. Показано, что представленная оптимизационная задача относится к классу задач безусловного нелинейного программирования с непрерывными переменными. Обосновано, что для решения такого типа задач целесообразно применять процедуры природных вычислений [2, с. 8 – 12], которые лежат в основе предложенного метода построения нерегулярных кодов с малой плотностью проверок на четность. Для оценки эффективности предложенного подхода к построению данного класса помехоустойчивых кодов разработаны вычислительные алгоритмы и соответствующая программная реализация телекоммуникационной системы в специализированной среде моделирования. Приведены полученные распределения степеней символьных и проверочных вершин графа Таннера и соответствующие проверочные матрицы нерегулярных кодов с малой плотностью проверок на четность.

Литература
1. Gallager, R. G. Low-density parity-check codes / R. G. Gallager // IRE Transaction on Information Theory. – 1962. – January. – P. 21 – 28.
2. Карпенко, А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой [Текст]: учебное пособие / А. П. Карпенко. – М: издательство МГТУ им. Н. Э. Баумана, 2014. – 446 с.

***Щербина Ю.В.**, к.т.н, доцент,*
***Фразе-Фразенко А.А.**, к.т.н.,*
Одесский национальный экономический университет,
г. Одесса, Украина

ПОДХОД К ПОСТРОЕНИЮ ВЫСОКОСКОРОСТНЫХ ВЫЧИСЛИТЕЛЬНО-СТОЙКИХ ШИФРОВ НА ОСНОВЕ ПРОСТЫХ КОНГРУЭНТНЫХ ГЕНЕРАТОРОВ

Обсуждается вопрос о построении поточных шифров. Для построения высокоскоростных вычислительно-стойких шифров предлагается использовать простые конгруэнтные генераторы. На этой основе строятся генераторы, которые дают четное число последовательностей. Показано, что равномерность последовательностей испытана и не вызывает сомнения. Датчики, которые входят в состав генератора, выбираются так, что их периоды являются наибольшими. Выходы датчиков объединяются попарно в мультипликативно-аддитивные группы. Объединение выполняется так, что на выходах датчиков формируются однобайтовые комбинации. Это обеспечивает удобство реализации процедур гаммирования в процессе шифрования.

Генерация программными методами истинно случайных последовательностей для криптографических нужд, изначально созданных как детерминированные устройства, является невыполнимой задачей. Использование для этой цели физических генераторов шумов дорого и неудобно. По этой причине инженерные усилия в настоящее время сосредоточены на построении функций, выдающих серии чисел, обладающих необходимыми свойствами и проходящие ряд тестов на случайность.

Для обеспечения безопасности компьютерных систем критически важно иметь алгоритмы, удовлетворяющие следующим условиям:

–последовательности должны проходить предусмотренные тесты на случайность;

–формируемый поток чисел должен обладать содержательной непредсказуемостью.

Критериям надёжности в настоящее время уделяется большое внимание, поскольку «слабые» случайные последовательности позволяют потенциальным нарушителям вскрывать заложенные в алгоритмах их формирования принципы и на этой основе организовывать эффективные атаки на ключевую систему.

Созданные на данный момент генераторы проектировались с учетом состояния вычислительной техники своего времени. Рост вычислительных ресурсов современных электронно-вычислительных машин (ЭВМ), позволяет существенно повысить качество формируемых псевдослучайных последовательностей (ПСП). Эта задача особенно актуальна, поскольку спектр известных алгоритмов не особенно широк. Так сложилось, что до настоящего времени датчики случайных чисел разрабатывались авторами в индивидуальном порядке для каждого конкретного криптографического продукта. С учетом того, что криптографы не особенно охотно делятся с коллегами своими достижениями, общая теория формирования ПСП требует дальнейшего изучения и разработки.

Псевдослучайная последовательность считается удовлетворительной, если на основании наблюдения достаточно длинной последовательности ранее принятых символов невозможно предсказать значение следующего символа с вероятностью, отличной от $p = 0{,}5$.