Математическое и компьютерное моделирование:
материалы III Международной научной конференции
(Омск, 12 ноября 2015 г.). Омск, 2015. С. 187–188. УДК 004.9

В.С. Виноградов, В.В. Коробицын, М.Н. Московцев

Омский государственный университет им. Ф.М. Достоевского, г. Омск

ИСПОЛЬЗОВАНИЕ ТУРБО-КОДЕКА ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ

В современных информационных системах, связанных с передачей информации по различным каналам связи, очень остро строит вопрос обеспечения информационной безопасности передаваемых данных. При этом коммуникационные технологии в определенных условиях должны работать в средах с низким соотношением сигнал-шум, что обеспечивает необходимость использования помехоустойчивого кодирования. Одним из наиболее востребованных на настоящий момент классов помехоустойчивых кодов является класс турбо-кодов. В работе предложен алгоритм защиты данных от несанкционированного доступа при передаче в каналах связи с помехами, основанный на алгоритмах класса турбо-кодов. Рассмотрены варианты использования подобного алгоритма, эффективность прикладной реализации, а также вспомогательная информационная инфраструктура для разработанного метода, например, алгоритм генерации ключей.

Было предложено в качестве ключа использовать зерно, а также внутренние параметры генератора. Очевидны следующие проблемы: параметры генератора подобраны специальным образом для максимальной эффективности алгоритма генерации псевдослучайных последовательностей. Поэтому использование случайных значений параметров не является эффективным. Длина ключа в 32 бита (ключ – зерно одного генератора) для современных алгоритмов не считается достаточной, поскольку позволяет осуществить взлом методом полного перебора за ограниченное время. Учитывая изложенные обстоятельства, от подобного подхода построения ключа было решено отказаться.

Был разработан алгоритм построения ключа, основанный на тех же принципах генерации перестановки перемежителя, которые использовались ранее. Суть алгоритма заключается в использовании

нескольких генераторов псевдослучайных чисел. При этом ключ для алгоритма формируется с помощью конкатенации зерен каждого генератора в бинарном виде.

Полученный ключ имеет следующие свойства:

1. Минимальная длина ключа – 64 бита. Данная особенность возникает из необходимости иметь как минимум 2 генератора псевдослучайных последовательностей с разным инициализирующим зерном. Это свойство не накладывает существенных ограничений на использование алгоритма.

2. Длина ключа должна быть кратна 32 битам.

3. Длина ключа сверху никак не ограничивается алгоритмом, но при этом необходимо отметить, что использование слишком больших ключей не является целесообразным.

При этом подобный алгоритм легко поддается распараллеливанию, что является очень удобным для организации системы управления ключами. Таким образом, с помощью алгоритмов параллельных вычислений можно формировать банки ключей для подобных систем связи.

Литература

1. An Investigation of Code Matched Interleaver for 3G Turbo Code Systems. URL: http://www.researchgate.net/profile/Balamuralithara_Balakrishnan/publication/26560302_An_Investigation_of_Code_Matched_Interleaver_for_3G_Turbo_Code_Systems/links/00b4953070a93a2ce3000000.pdf .

2. Особенности стандарта LTE. URL: http://cmpo.vlsu.ru/edu/2013/A7.pdf.

3. Спецификация DVB-RCS. URL: https://www.dvb.org/resources/public/factsheets/DVB-RCS2_Factsheet.pdf.

4. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005.

5. Метод перемешивания Байеса-Дарема. URL: http://en.wikibooks.org/wiki/Statistics/Numerical_Methods/Random_Number_Generation#Bays-Durham_Shuffling_of_Uniform_Deviates.