СКРЕМБЛИРОВАНИЕ ЗАШУМЛЕННЫХ СООБЩЕНИЙ В МНОГОЯДЕРНОЙ ВЫЧИСЛИТЕЛЬНОЙ СРЕДЕ

И.П. Кобяк

В представляемой работе рассмотрен метод нахождения детерминизма в зашумленных сообщениях с использованием многоядерных процессоров. Сущность метода заключается в декомпозиции последовательности T^n из n символов на m подмножеств с последующим удалением шума в каждом из подмножеств. Вновь сформированные последовательности E^m рассматривается как кодированные сообщения некоторого выбранного языка с фиксированной длиной букв равной l ($l = l_1, l_2, \ldots$). За каждым из m подмножеств символов закрепляется свое ядро многоядерной системы, реализующее функцию раскодирования. На шаге два наборы двоичных бит E^m проверяется на принадлежность кодировкам заданного языка из таблицы t_k всевозможных кодов символов с 2^l ячейками. При совпадении символов и кодов формируется буквенное слово, которое записывается в свой слот общего фрейма системы. В качестве фрейма используется виртуальный объект, состоящий из m призм с s гранями. При этом каждая i-я ($i = 1, 2, \ldots, s$) грань призмы длиной m является слотом соответствующего ядра процессора. Под действием алгоритма выполняется заполнение слотов всех призм фрейма. Далее осуществляется программное «вращение» призм друг относительно друга с выбором лингвистической подсистемой некоторого «осмысленного» сообщения, что соответствует приведенному в [1] алгоритму скремблирования. Положительным моментом представленной системы является параллельное формирование шумов, приводящее к сокращению времени в фазе преобразования $T^n \rightarrow E^m$ с $f(2^n)$ до $f(2^m)$. Максимальное же время «лингвистического» вращения в составе фрейма определяется как $f(s^m)$.

Литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ. 2001. 480 с.