

Секция 5

**ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ
В ДИСКРЕТНОЙ МАТЕМАТИКЕ**

УДК 519.7

**РЕШЕНИЕ ЗАДАЧ КРИПТОАНАЛИЗА В ГРИД-СИСТЕМАХ
(НА ПРИМЕРЕ BOINC)¹**

О. С. Заикин

Логический криптоанализ (постановка задачи криптоанализа как задачи поиска выполняющих наборов пропозициональных выражений) показал свою перспективность в отношении некоторых систем поточного шифрования. Основы крупноблочной параллельной технологии решения SAT-задач описаны в [1]. Реализация данной технологии в виде параллельного SAT-решателя PD-SAT с использованием библиотеки MPI представлена в [2]. С применением решателя PD-SAT были успешно решены на вычислительных кластерах задачи логического криптоанализа суммирующего генератора, порогового генератора, а также генератора Гиффорда (с длинами ключей 66, 80, 64 бит). Логический криптоанализ генератора A5/1 потребовал весьма значительных вычислительных ресурсов, получение которых в рамках одного (пусть даже очень мощного) вычислительного кластера, как правило, проблематично. В связи с этим было принято решение о переносе технологии распараллеливания SAT-задач в распределенные вычислительные среды. Первым удачным опытом такого рода стало успешное решение задач криптоанализа генератора A5/1 в грид-системе BNB-Grid [3].

В настоящее время большое число исследований посвящено решению трудных комбинаторных задач в так называемых Desktop-Grid — грид-системах, в которых в роли вычислительных узлов выступают обычные персональные компьютеры (ПК). Принцип организации таких грид-систем заключается в предоставлении пользователями ресурсов своих ПК на добровольной основе. Наиболее популярной платформой для организации Desktop-Grid является Berkeley Open Infrastructure for Network Computing (BOINC, [4]). Пользователь устанавливает клиент BOINC, с помощью которого подключается через Интернет к проекту, после чего ПК начинает получать и обрабатывать задания. Режим обработки заданий гибко настраивается (по умолчанию обработка заданий начинается, когда ПК некоторое время не используется). Существуют проекты на основе BOINC, объединяющие сотни тысяч ПК (например, проект поиска радиосигналов внеземных цивилизаций SETI@home).

Реализована новая грид-версия решателя PD-SAT, предназначенная для использования в проектах на основе платформы BOINC. Для этой цели использована библиотека DC-API [5]. Применение PD-SAT позволило успешно решить в рамках BOINC-проекта задачи криптоанализа ряда генераторов (суммирующего, порогового, генератора Гиффорда). В ближайшее время планируется организовать BOINC-проект, состоящий из нескольких тысяч ПК для решения более масштабных задач криптоанализа.

¹Работа поддержана грантом «Лаврентьевский конкурс молодежных проектов СО РАН» 2010–2011 гг. и грантом РФФИ, проект № 11-07-00377-а.

ЛИТЕРАТУРА

1. Заикин О. С., Семенов А. А. Технология крупноблочного параллелизма в SAT-задачах // Проблемы управления. 2008. № 1. С. 43–50.
2. Заикин О. С. Реализация процедур прогнозирования трудоемкости параллельного решения SAT-задач // Вестник УГАТУ. 2010. Т. 14. № 4(39). С. 210–220.
3. Посыпкин М. А., Заикин О. С., Беспалов Д. В., Семенов А. А. Решение задач криптоанализа поточных шифров в распределенных вычислительных средах // Труды ИСА РАН. 2009. Т. 46. С. 119–137.
4. <http://boinc.berkeley.edu> — Berkeley Open Infrastructure for Network Computing.
5. <http://www.desktopgrid.hu> — SZTAKI desktop grig.

УДК 519.7

**BOOLEAN FUNCTIONS — СИСТЕМА ДЛЯ РАБОТЫ
С БУЛЕВЫМИ ФУНКЦИЯМИ¹**

Н. А. Коломеец, А. В. Павлов

Предлагается новая система для работы с булевыми функциями *Boolean Functions*. Эта система ориентирована на пользователей-программистов и представляет собой библиотеку классов и функций на языке C++; она может быть полезна для проведения компьютерных экспериментов и тестов, связанных с булевыми функциями. В отличие от других систем, таких, как MAGMA, система является узконаправленной на работу с булевыми функциями специального вида. Кроме того, *Boolean Functions* бесплатна и свободно распространяема.

Для решения многих математических задач требуется подготовка экспериментальной базы и проведение компьютерных тестов. Каждый раз для новой подобной задачи приходится заново создавать все вспомогательные функции, такие, как проверка принадлежности функции какому-либо классу или перевод функции в различные представления (АНФ, таблица истинности, трейс-форма). Предлагаемая система предназначена для сокращения этих действий. На данный момент *Boolean Functions* является весьма неполной системой, хотя и содержит некоторые готовые алгоритмы; предполагается дальнейшее её развитие и выпуск новых версий.

Система позволяет работать с двоичными векторами и совершать стандартные операции над ними, такие, как определение веса Хэмминга, сложение двух векторов, вычисление их скалярного произведения, сравнение двух векторов и др.

Библиотека работает с представлениями булевой функции в виде АНФ, таблицы истинности и представлением с помощью следа (трейс-форма), а также умеет переводить одно представление в другое.

Boolean Functions позволяет проверять, являются ли две булевы функции аффинно эквивалентными (используется алгоритм [1]), а также генерировать функции, аффинно эквивалентные заданной.

Основное предназначение данной системы — работа с булевыми функциями специального вида, в частности с бент-функциями. Система позволяет проверять, является ли булева функция бент-функцией. *Boolean Functions* содержит алгоритмы генерации бент-функций от 4, 6 и 8 переменных степени не больше 3, алгоритм генерации

¹Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0362).