Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ, СТЕГАНОГРАФИИ И КОДИРОВАНИЯ

УДК 519.7

ГИБРИДНЫЙ ПОДХОД (SAT+ROBDD) В ЗАДАЧАХ КРИПТОАНАЛИЗА ПОТОЧНЫХ СИСТЕМ ШИФРОВАНИЯ

А. С. Игнатьев, А. А. Семенов, Д. В. Беспалов, О. С. Заикин

В настоящем докладе представлен подход к решению логических (булевых) уравнений, в основе которого лежит гибридная стратегия, использующая как быстрые алгоритмы решения SAT-задач (нехронологический DPLL-вывод), так и двоичные диаграммы решений (BDD). Построенные алгоритмы тестировались на задачах обращения ряда криптографических функций.

Главным объектом рассмотрения являются задачи обращения всюду определенных дискретных функций, вычислимых за полиномиальное время. Более точно, речь идет о семействах функций вида $f_n : \{0,1\}^n \to \{0,1\}^*$, где $\{0,1\}^n$ — множество всевозможных двоичных векторов длины n, а $\{0,1\}^*$ — множество всевозможных двоичных векторов произвольной конечной длины. Предполагается, что для любого $n \in N$ функция f_n всюду определена и существует программа для детерминированной машины Тьюринга (ДМТ), которая вычисляет все функции семейства $f = \{f_n\}_{n \in N}$. Если такая программа имеет полиномиальную от n сложность, то говорим, что семейство функций f находится в классе $\Im$. Задача обращения $f_n \in \Im$ заключается в том, чтобы по известному y из области значений f_n найти такое $x \in \{0,1\}^n$, что $f_n(x) = y$.

В работах [1 – 4] был развит пропозициональный подход к задачам обращения дискретных функций из класса $\Im$. В основе данного подхода лежит идея пропозиционального представления алгоритмов, восходящая к С. А. Куку. В соответствии с пропозициональным подходом алгоритм вычисления дискретной функции $f_n \in \Im$ представляется в виде системы логических уравнений $S(f_n)$, которая, грубо говоря, описывает все возможные варианты эволюции программы, вычисляющей f_n, на входах из $\{0,1\}^n$. После подстановки в систему $S(f_n)$ вектора y из области значений f_n имеем совместную систему логических уравнений $S(f_n)|_y$, решая которую, находим такой $x \in \{0,1\}^n$, что $f_n(x) = y$. Для решения систем вида $S(f_n)|_y$ могут использоваться различные подходы. В [1 – 4] для этих целей применялся SAT-подход, в основе которого лежит техника приведения систем $S(f_n)|_y$ к уравнениям вида «КНФ=1».

В [3] была предложена технология крупноблочного параллелизма, предназначенная для решения SAT-задач. В работах [1, 3, 4] данная технология использовалась для решения задач обращения некоторых криптографических функций на суперкомпьютерах.

В качестве новых результатов в настоящем докладе фигурирует описание комбинированного подхода к решению задач обращения дискретных функций из класса $\Im$, использующего как SAT-технологии, так и двоичные диаграммы решений (BDD). Основная идея такого подхода состоит в использовании BDD, а точнее, ROBDD для модификации баз конфликтных дизъюнктов. Соответствующий механизм позволяет

избежать потери полноты базовым алгоритмом решения SAT-задачи (данный негативный эффект, возникающий в современных SAT-решателях, был отмечен в [4]). Предполагается рассмотреть результаты вычислительных экспериментов по использованию гибридного подхода (SAT+ROBDD) в распределенных вычислительных средах.

ЛИТЕРАТУРА

1. *Семенов А. А., Заикин О. С., Беспалов Д. В. и др.* Решение задач обращения дискретных функций на многопроцессорных вычислительных системах // Труды Четвертой Междунар. конф. «Параллельные вычисления и задачи управления» PACO'2008, Москва, 26–29 октября 2008. 2008. С. 152–176.
2. *Семенов А. А., Заикин О. С., Беспалов Д. В., Ушаков А. А.* SAT-подход в криптоанализе некоторых систем поточного шифрования // Вычислительные технологии. 2008. Т. 13. № 6. С. 134–150.
3. *Заикин О. С., Семенов А. А.* Технология крупноблочного параллелизма в SAT-задачах // Проблемы управления. 2008. № 1. С. 43–50.
4. *Семенов А. А., Заикин О. С.* Неполные алгоритмы в крупноблочном параллелизме комбинаторных задач // Вычислительные методы и программирование. 2008. Т. 9. № 1. С. 112–122.

УДК 681.3+519.71

ОБОБЩЕННАЯ ОБРАТИМОСТЬ ДИНАМИЧЕСКИХ СИСТЕМ В ЗАДАЧАХ ШИФРОВАНИЯ

А. М. Ковалев, В. А. Козловский, В. Ф. Щербак

Рассматривается метод преобразования оцифрованной информации, основанный на дискретной динамической системе, порождающей передаточное отображение: вход (информационное сообщение) — выход (закодированное сообщение). Восстановление входа осуществляется с помощью специальным образом построенной обратной системы. Предложены конструкции обратимых систем, обладающие различной степенью обратимости: обратимые, идентифицируемые и обратимые на множестве траекторий. Рассмотрены конечно-автоматные конструкции, реализующие указанный подход.

Пусть передача информации осуществляется с помощью дискретной динамической системы, правые части которой зависят от вектор-функции $u(.)$ — оцифрованного информационного сообщения:

$$x(k+1) = f(x(k), u(k)), \quad x(0) = x_0, \tag{1}$$

$$y(k) = h(x(k), u(k)), \quad y \in R^m, \tag{2}$$

где $x(.) \in R^n$, $u(.) \in R^m$, $y(.) \in R^m$ определяют векторы состояния системы, ее вход и выход соответственно. По каналам связи передается выходной сигнал — функция $y(k)$, зависящая от состояния системы, ее параметров и сообщения $u(k)$. Рассматривается задача восстановления значений входного воздействия по значениям функции выхода. В теории управления непрерывными динамическими системами одним из способов ее решения является построение системы, обратной к исходной [1, 2]. Базовым свойством таких систем является обратимость. В терминах теории управления динамические системы, пригодные для преобразования и передачи информации, составляют класс обратимых систем управления. При этом многомерность динамической системы, наличие сложных взаимосвязей между переменными позволяют конструировать системы