УДК 004.056

В.И. Дулькейт, Р.Т. Файзуллин, И.Г. Хныкин

Минимизация функционалов, ассоциированных с задачами криптографического анализа

Описывается способ решения задачи ВЫПОЛНИМОСТЬ (SAT) путем минимизации ассоциированного функционала специального вида. Показаны практические применения приведенных алгоритмов в задачах асимметричного криптоанализа.
Разработан генератор задач асимметричного криптоанализа в виде задачи SAT.

Допустим $K(x)$ – пропозициональная формула в конъюнктивной нормальной форме на множестве переменных $x = \{x_1 \dots x_N\}$. Задача ВЫПОЛНИМОСТЬ заключается в том, чтобы найти решающий набор $x_0 = \{x_1 = L_1 \dots x_k = L_k / L_i = 0,1\}$, такой что $K(x_0) = 1$, или доказать, что решающего набора не существует.

Переход от задачи ВЫПОЛНИМОСТЬ к задаче поиска глобального минимума функционала вида происходит по формуле [3]:

(1)

Ошибка! Объект не может быть создан из кодов полей редактирования.

Здесь $C_i(x)$ – дизъюнкты 3-КНФ, эквивалентной исходной КНФ. Суммирование ведется по всем M конъюнктам эквивалентной 3-ДНФ. Соответствие между булевыми и вещественными переменными следующее: ЛОЖЬ→0, ИСТИНА→1. При этом $\min\limits_{x \in E^N} F(x) = 0$ соответствует достижению значения ИСТИНА на исходной КНФ.

Дифференцируя функционал (1) по всем переменным x_i, получим систему уравнений:

$$\sum_{\xi \in \Xi} z_j^2 z_k^2 x_i = \sum_{\xi \in \Lambda} z_j^2 z_k^2 \underset{def}{\sim} A_i x_i = B_i,\ i = 1,..P, \text{ где } z_i = \begin{cases} 1 - x_i, \text{если } x_i \in C_i(x), \\ x_i \quad, \text{если } \bar{x}_i \in C_i(x). \end{cases}$$

$$\Xi = \{\xi,\ i \in \xi : \bar{x}_i \in C_i(x)\},\ \Lambda = \{\xi,\ i \in \xi : x_i \in C_i(x)\}. \quad (2)$$

Поясним выбор представления исходной КНФ именно в виде эквивалентной 3-ДНФ. Дифференцируя функционал $F(x)$ по всем переменным x_i, получаем систему уравнений (2), но количество вкладов в A_i и B_i определяется длиной скобок. Любая процедура решения этой системы при произвольной длине скобок будет естественным образом приводить к большим ошибкам округления. Ограничивая число переменных в скобках, мы исключаем эту техническую трудность.

Для решения системы предлагается метод последовательных приближений с «инерцией»:

$$\left(\sum_{p=0}^{K} \alpha_p \sum_{\xi \in \Xi} p_\xi z_i(t-p)^2 z_j(t-p)^2 \right) x_k(t+1) = \sum_{\xi \in \Lambda} z_j^2(t) z_k^2(t) \underset{def}{\approx} A \cdot x_k(t+1) = B,$$

$$\sum_{p=1}^{K} \alpha_p = 1, \text{ где } \alpha_p \in R[0,1],\ p_\xi \geq 0.$$

Итерации проводятся для вещественных чисел (используется метод Зейделя), а итоговый, или промежуточный, вектор проектируется на $B^N\{0,1\}$, и на булевом векторе проверяется SAT.

Для улучшения сходимости метода разработаны различные модификации: метод резолюции, сдвиг по градиенту, метод смены траектории, введение весов по вхождению переменных.

Для тестирования метода был разработан генератор задач криптоанализа асимметричных шифров – факторизации, дискретного логарифмирования, дискретного логарифмирования на эллиптической кривой в виде задачи ВЫПОЛНИМОСТЬ. Исходная задача разлагается на элементарные операции, для которых строится соответствующая булева формула. Затем эти формулы объединяются в результирующую КНФ. Подробно способ генерации описан в [1].

При тестировании использовались примеры библиотеки SATLib, примеры больших размерностей, сформированные случайным образом, примеры, сформированные для задачи факторизации. Числа для задачи факторизации брались с учетом всех требований, предъявляемых к алгоритму RSA.

Вычислительные эксперименты для примеров SATLib, показали сравнимые с ведущими алгоритмами результаты. При тестировании примеров сформированных случайно показано, что при $N / M \leq 0,5$, где N это число переменных, M – число дизъюнктов в КНФ, итерационная процедура

всегда сходится к решению. Для примеров, эквивалентных задаче факторизации удается найти решение задач размерности до 72 бит за время менее 200 часов, что превосходит результаты алгоритмов, представленных на соревнованиях 2005 года (www.cs.ubc.ca/~hoos/) [2].

Для задачи факторизации получен интересный результат. Уже после нескольких сотен итераций метод позволяет находить более 65% неизвестных (рис. 1). Причем найденные неизвестные являются ключевыми для решения задачи, т.е. после подстановки их значений в исходную формулу, последняя легко разрешается. Другой интересный результат в том, что с ростом размерности задачи процент верных бит логарифмически возрастает. На рисунке представлены результаты расчетов для серий задач, средние значения верных бит, наилучшая аппроксимация логарифм по методу наименьших квадратов, и соответствующие максимальные значения.

Рис. 1. Зависимость процента числа верных бит от размерности задач

Учитывая, что многие задачи криптографического анализа могут быть представлены в булевой форме, с последующим сведением их к задаче минимизации функционала представляется перспективным применение представленной методики, во всяком случае, для решения задач дискретного логарифмирования и логарифмирования на эллиптической кривой. Предварительные результаты для этих задач аналогичны результатам для задачи факторизации.

Литература

1. Дулькейт В.И., Файзуллин Р.Т., Хныкин И.Г. Алгоритм минимизации функционала, ассоциированного с задачей 3-SAT, и его практические применения // ПаВТ. – Челябинск, 2006.

2. Хныкин И.Г. Алгоритм минимизации функционала, ассоциированного с задачей SAT // Кунгурка – 2008.

3. Gu J., Purdom P.W., Franco J., Wah B.W. Algorithms for the Satisfiability Problem: A Survey // DIMACS Series in Discrete Mathematics and Theoretical Computer Science. – 1996. – С. 19–151.

Дулькейт Владимир Игоревич
ГОУ ВПО Омский государственный университет им. Ф.М. Достоевского, аспирант

Файзуллин Рашит Тагирович
ГОУ ВПО Омский государственный университет им. Ф.М. Достоевског
Д.т.н., профессор, зав. кафедрой комплексных систем защиты информации

Хныкин Иван Геннадьевич
ГОУ ВПО Омский государственный университет им. Ф.М. Достоевского, аспирант
Эл. почта: r.t.faizullin@mail.

V.I. Dulkeyt, R.T. Faizullin, I.G. Khnikin

Global optimization problems associated with cryptographic analysis of asymmetric ciphers

The aim of this article is to establish relation between well-known problems of cryptographic analysis and global optimization problems which can be associated with SAT representation of cryptographic algorithms where bits of key is part of SAT solution string. There was constructions SAT forms for factorization problem, SAT forms for logarithmic problem and logarithmic problem on elliptic curves. For numerical solution was adapted some low relaxation algorithms and for example results of numerical experiments give to us strong more then 50% bits for unknowns in SAT factorization form.