Рассмотрим общий случай, не предполагающий специальной структуры матрицы. Воспользуемся тем, что матрица симметрична и спектр ее вещественный, тогда можно записать

$$y = \sum_{i=1}^{N} \alpha_i v_i,$$

где v_i — это собственные векторы, отвечающие собственным числам, определяемым из уравнения

$$Bv_i = \lambda_i v_i. \tag{4}$$

Здесь λ_i могут быть равны нулю. Правая часть системы (3) представляется в виде

$$g = \sum_{i=1}^{N} \lambda_i \alpha_i v_i.$$

В итоге верна следующая теорема.

Теорема. Компоненты кортежей $(\alpha_1, .., \alpha_N)$, на которых достигается равный нулю минимум функционала

$$J(\alpha_1, ..., \alpha_N) = \sum_{j=1}^{M} \prod_{q=1}^{3} C_j^q + I(\alpha_1, ..., \alpha_N),$$

$$C_j^q = (q - \sum_{\xi \in \Xi_j} \Theta^{\xi q})^2,$$

$$\Xi_j = (i_1, i_2, i_3, \tau_1, \tau_2, \tau_3),\ \tau_t = 1 \vee 0, \quad i_t \in \{1, ..., N\},$$

$$\Theta^{\xi q} = \sum_{s=1}^{3} (-1)^{\tau_s} (y_{i_s} - \tau_s),$$

$$y_{i_s} = \sum_{w=1}^{N} \alpha_w v_{wi_s},$$

$$I(\alpha_1, ..., \alpha_N) = \sum_{z=1}^{N} y_z^2 (1 - y_z)^2,$$

являются коэффициентами разложения решения задачи ВЫПОЛНИМОСТЬ $y = \sum_{i=1}^{N} \alpha_i v_i$, где индекс w при v индексирует номер собственного вектора, множество индексов Ξ_j — это номера литералов, входящих в j-й дизъюнкт, и отвечающие им индексы τ, определяющие, как входит литерал в дизъюнкт, с отрицанием или без него.

Данные результаты позволяют для некоторых классов задач определять четверть части решающего набора для 3-SAT с вероятностью, равной или больше 0,9.

УДК 519.7

ЭКВИВАЛЕНТНОЕ ПРЕОБРАЗОВАНИЕ КНФ, АССОЦИИРОВАННЫХ С ЗАДАЧАМИ КРИПТОГРАФИЧЕСКОГО АНАЛИЗА, С ПОМОЩЬЮ ПРАВИЛ РЕЗОЛЮЦИИ

И. Г. Хныкин

Одним из методов криптоанализа является логический криптоанализ, когда криптографический алгоритм рассматривается как программа для машины Тьюринга и

подстановка открытого и шифрованного текстов в эту программу приводит к задаче ВЫПОЛНИМОСТЬ (SAT) для КНФ. Проблема состоит в том, что получаемые КНФ имеют большие размерности даже при небольшой размерности исходной задачи. Представленный в данной работе метод позволяет преобразовать исходную КНФ в эквивалентную, с меньшим количеством дизъюнктов и переменных. Метод может быть использован как препроцессор КНФ для увеличения эффективности алгоритмов решения задачи SAT [1].

Метод резолюции основан на правилах исчисления высказываний и включает в себя ряд методик.

1. *Простая резолюция и разрешение уникальных переменных*. Данная методика основана на следующих правилах вывода:

1) $(x \vee Y)\&x \Leftrightarrow Y$
2) $\text{TRUE} \vee x \Leftrightarrow \text{TRUE}$
3) $\text{FALSE} \vee x \Leftrightarrow x$
4) $x \vee x \Leftrightarrow \text{TRUE}$
5) $x\&x \Leftrightarrow$ o (пустой дизъюнкт)

2. *Резолюция по соседним дизъюнктам*. Два дизъюнкта называются соседними, если они различаются знаком по единственному литералу. Резольвентой по соседним дизъюнктам называется дизъюнкт, являющийся максимальным общим подмножеством соседних дизъюнктов. Если в КНФ присутствует конъюнкция соседних дизъюнктов, то конъюнкция заменяется резольвентой по соседним дизъюнктам.

3. *Бинарная резолюция*. Два дизъюнкта разрешимы относительно бинарной резолюции (бинарно разрешимы), если они совпадают хотя бы по одной переменной, которая входит в один дизъюнкт с отрицанием, а в другой — без.

Справедлива следующая теорема, которая показывает, что бинарная резолюция в применении к исходной КНФ может дать тот же результат, что и резолюция по соседним дизъюнктам, периодически применяемая во время поиска решения.

Теорема 1. Любой дизъюнкт, полученный в результате резолюции по соседним дизъюнктам в процессе переборного поиска решения, является производным от некоторого дизъюнкта, который может быть получен в результате применения бинарной резолюции к исходной КНФ.

В результате применения методик 1–3 количество дизъюнктов в КНФ уменьшается, что приводит к уменьшению области поиска для различных алгоритмов решения задачи SAT.

Для проведения численных экспериментов были использованы следующие классы КНФ: FACTOR (КНФ, ассоциированные с задачей факторизации), DLOG (КНФ, ассоциированные с задачей дискретного логарифмирования), EDLOG (КНФ, ассоциированные с задачей дискретного логарифмирования на эллиптической кривой) [2]. Входные параметры алгоритмов сведения задач криптоанализа выбирались исходя из рекомендуемых соответствующими стандартами условий обеспечения криптостойкости [3]. Количество дизъюнктов и переменных в тестовых КНФ достигает 10^7 и 10^6 соответственно.

Результаты показывают, что для КНФ, ассоциированных с задачей факторизации, удается разрешать до 1,1 % переменных и сокращать до 67 % дизъюнктов исходной КНФ, независимо от размерности исходной задачи. Для КНФ, ассоциированных с остальными задачами криптоанализа, удается сократить число дизъюнктов на два

порядка. При этом трудоемкость метода резолюции не выше кубической от количества бит в ключе.

Таким образом, метод резолюции является эффективным препроцессором КНФ, ассоциированных с задачами криптоанализа асимметричных шифров.

ЛИТЕРАТУРА

1. *Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г.* Алгоритм минимизации функционала, ассоциированного с задачей 3-SAT, и его практические применения // Компьютерная оптика. 2008. Т. 32. № 1. С. 68–73.
2. *Дулькейт В. И.* КНФ-представления для задач факторизации и дискретного логарифмирования // Проблемы теоретической и прикладной математики: Труды 38-й Региональной молодежной конференции. Екатеринбург: УрО РАН, 2007. С. 350–355.
3. `www.rsasecurity.com` — RSA, The Security Division of EMC — Security Solutions for Business Acceleration