$a^{z_1} = g^{y \cdot z_1} = g^{y_1 \cdot s \cdot z_1} = g^{y_1 \cdot z} = b^{y_1} (\mathrm{mod}\, p)$, откуда получаем $x = \log_a b = z_1 \cdot y_1^{-1} \mathrm{mod}\, q$. Здесь $y_1^{-1} \mathrm{mod}\, q$ всегда существует в силу условия $0 < y_1 < q$.

При таком подходе нужно дважды решать задачу логарифмирования в $\mathbb{Z}_p^*$, что предполагает решение двух систем линейных уравнений над кольцом, в то время как в методе [2] решается одна система линейных уравнений над полем. Что касается ограничения $(q, s) = 1$, то это условие автоматически выполнено, если простое p построено методом Маурера (так как в этом случае $s < q$), и выполнено с вероятностью $(q-1)/q$, если p построено по алгоритму ГОСТ (поскольку s — случайное число в некотором диапазоне, в котором каждое q-е число кратно q). Таким образом, в большинстве случаев задачу логарифмирования в числовой группе G простого порядка можно решать методом Адлемана, не требуя выбора факторной базы как подмножества G.

ЛИТЕРАТУРА

1. *Menezes A. J., Van Oorshot P. C., Vanstone S. A.* Handbook of Applied Cryptography. N. Y.: CRC Press Series on Discrete Mathematics and Its Applications, 1997.
2. *Белов А. Г.* Исследование алгоритма дискретного логарифмирования Адлемана // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 45–49.

УДК 519.7

ЗАДАЧИ ЛИНЕЙНОЙ АЛГЕБРЫ, СООТНЕСЕННЫЕ С ЗАДАЧЕЙ ВЫПОЛНИМОСТЬ

Р. Т. Файзуллин

Рассмотрим переход от задачи 3-ВЫПОЛНИМОСТЬ к задаче решения систем линейных алгебраических уравнений. Пусть дана КНФ:

$$L(x) = \prod_{i=1}^{M} C_i, \tag{1}$$

где C_i — дизъюнкты вида $\vee q_{ij}$. Здесь $q_{ij} = x_j$ или $q_{ij} = \bar{x}_j$.

Заметим, что каждому дизъюнкту можно поставить в соответствие уравнение, связывающее уже вещественные переменные. В правой части стоят единицы, а переход от булевых переменных к вещественным осуществляется согласно формулам: $x_j \to y_j$, $\bar{x}_j \to 1 - y_j$. В этом случае мы получаем систему линейных алгебраических уравнений с прямоугольной матрицей:

$$Ay = f. \tag{2}$$

Обратим внимание на то очевидное обстоятельство, что правая часть f_j равна количеству q_{ij}, принимающих значение ИСТИНА в исходной КНФ. Систему можно преобразовать согласно формуле

$$RAy = Bf = Rf = g. \tag{3}$$

Попытаемся построить матрицу B таким образом, чтобы получить в итоге симметричную матрицу. Рассмотрим переменную с индексом j и соответствующие ей уравнения в (3). Будем складывать эти уравнения, аккумулируя неизвестные в j-й строке B, умножая их на -1, если переменная входит в уравнение со знаком минус. Тогда верна следующая лемма.

Лемма. Итоговая матрица B симметрична.

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