# Сведение задач криптоанализа асимметричных шифров к решению ассоциированных задач «ВЫПОЛНИМОСТЬ»

***Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г.***
r.t.faizullin@mail.ru, hig82@rambler.ru
Омск, Омский государственный университет им. Ф. М. Достоевского

Предложен способ решения задач криптоанализа асимметричных шифров (факторизации, дискретного логарифмирования) путем сведения к задаче ВЫПОЛНИМОСТЬ (SAT) и минимизации, специальным образом построенного, функционала.

Задача SAT заключается в поиске набора булевых значений, на котором заданная булева формула, представленная в КНФ, принимает значение ИСТИНА. Перспективным направлением в решении задачи SAT представляется её сведение к непрерывному аналогу, к задаче поиска точек глобального минимума ассоциированного с КНФ функционала [1]. В работе обосновывается выбор функционала специального вида. Предлагается применить к решению системы нелинейных алгебраических уравнений, определяющих стационарные точки функционала, модифицированный метод последовательных приближений.

Показано, что метод, в отличие от большинства существующих методов, позволяет достаточно эффективно находить решение для КНФ, эквивалентных указанным задачам криптоанализа. Рассматривается применимость метода к другим реальным задачам.

Сведение задач криптоанализа к задачам SAT осуществляется путем кодирования элементарных составляющих операции умножения и дискретного логарифмирования в терминах булевой алгебры. Метод кодирования представлен в работе [1].

### Построение модифицированного метода последовательных приближений

Пусть $K(x) = \bigcap_{i=1}^{M} C_i(x)$ — КНФ. Переход от задачи SAT к задаче поиска глобального минимума функционала осуществляется по формуле

$$\min_{x \in E^n} F(x) = \min_{x \in E^n} \sum_{i=1}^{M} \prod_{j=1}^{N} Q_{i,j}(x) = 0; \tag{1}$$

$$Q_{i,j}(x) = \begin{cases} (1 - x_j)^2, & \text{если } x_j \in C_i(x); \\ x_j^2, & \text{если } \bar{x}_j \in C_i(x); \\ 1, & \text{иначе.} \end{cases}$$

Легко заметить, что $\min\limits_{x\in E^n} F(x) = 0$ соответствует достижению значения ИСТИНА на исходной КНФ.

Дифференцируя функционал по всем $x_i$, получим систему уравнений:

$$\sum_{\xi\in\Xi}\prod_{j\neq i}^{N} Q_{i,j}(x)\cdot x_i = \sum_{\xi\in\Lambda}\prod_{j\neq i}^{N} Q_{i,j}(x) \text{ где } i = 1,\ldots,N; \tag{2}$$

$$\Xi = \{\xi, k\in\xi : x_i \text{ или } \bar{x}_i \in C_k(x)\}, \quad \Lambda = \{\xi, k\in\xi : x_i \in C_k(x)\}.$$

Для ее решения предлагается применить метод последовательных приближений с «инерцией»:

$$\left[\sum_{p=0}^{K}\alpha_p\sum_{\xi\in\Xi}\rho_\xi\prod_{j\neq i}^{N} Q_{i,j}(x(t-p))\right]\cdot x_i(t+1) = \sum_{\xi\in\Lambda}\prod_{j\neq i}^{N} Q_{i,j}(x(t-p)) \tag{3}$$

$$\sim A^i\cdot x_i(t+1) = B^i, \text{ где } \sum_{p=0}^{K}\alpha_p = 1, \quad \alpha_p \geqslant 0, \quad \rho_\xi \geqslant 0.$$

Положив в (3) $K = 0$, $\rho_\xi = 1$, получим простой метод последовательных приближений. В отличие от него, модифицированный метод формирует приближения не так быстро, что позволяет избегать областей притяжения аттракторов.

**Преобразование исходной КНФ методом резолюции**

Преобразование позволяет получить КНФ с меньшим количеством дизъюнктов и литералов, эквивалентную исходной.

Резольвента — дизъюнкция конъюнктов, отличающихся знаком по единственной переменной. Все возможные резольвенты добавляются к КНФ и используются для вычисления других резольвент. Дублирующие конъюнкты и тавтологии удаляются. Здесь используется сокращенная процедура с глубиной рекурсии 1. Вычислительная сложность процедуры $O(n\log n)$.

Метод резолюции в применении к КНФ, ассоциированных с задачами факторизации и дискретного логарифмирования позволяет уменьшить исходное число конъюнктов до 50% и разрешить до 20% переменных.

**Гибридизация и распараллеливание алгоритма.**

Гибридизация алгоритма состоит в добавлении дополнительных методов, позволяющих ускорить сходимость первоначального метода.

Основная процедура состоит из последовательных итераций, которые совмещают метод последовательных приближений (3) и сдвиг по градиенту: $x_i(t+1) = 2x_i(t) - B^i/A^i$, т.к. правая часть (2) суть градиент исходного функционала. Используется схема Зейделя.

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Размерность,бит | 40 | 44 | 52 | 56 | 60 |
| | Число литералов | 990 | 1199 | 1677 | 1946 | 2235 |
| | Число дизъюнктов | 22333 | 27291 | 38695 | 45141 | 52079 |
| | Время решения, м. | 7 | 36 | 360 | 36 | 612 |
| 2 | Размерность,бит | 18 | 20 | 22 | 24 | 26 |
| | Число литералов | 28224 | 38840 | 51832 | 67440 | 85904 |
| | Число конъюнктов | 448018 | 623239 | 839032 | 1099630 | 1409250 |
| | Время решения, с. | 63.57 | 108.20 | 182.73 | 277.46 | 417.71 |

**Таблица 1.** Результаты численных экспериментов: 1 — для задачи факторизации; 2 — для задачи дискретного логарифмирования.

Если скорость сходимости падает, применяется т. н. метод смены траектории. Текущее приближение проектируется на $B^n\{0,1\}$, и с некоторой вероятностью значения компонент вектора из множества $E = \{x_k \mid \exists$ конъюнкт $C_i\colon x_k$ или $\bar{x}_k \in C_i$ и $C_i(x) = 0\}$ меняются на противоположные. Работа алгоритма возобновляется с использованием нового полученного приближения.

Подробно о методах распараллеливания и ускорении сходимости: [1].

### Результаты численных экспериментов.

При тестировании использовались КНФ библиотеки SATLib (`satlib.org`) и КНФ, сформированные для задач факторизации и дискретного логарифмирования. Результаты для тестов SATLib сравнимы с результатами ведущих алгоритмов [1]. Тесты, сформированные для задач факторизации и дискретного логарифмирования, оказываются наиболее трудными. Ведущие алгоритмы (RANOV, SATz) не смогли за обозримое время найти решение уже для задачи факторизации размерности 40 бит.

Предложенный алгоритм показал приемлемый (предположительно субэкспоненциальный) рост времени решения и возможное наличие «слабых» примеров больших размерностей (табл. 1).

При модификациях простого метода последовательных приближений было достигнуто равномерное улучшение сходимости по всем тестам.

Был разработан способ генерации трудных для решения КНФ, основанных на задачах криптоанализа.

Учитывая, что многие реальные задачи могут быть представлены в булевой форме, представляется перспективным применение параллельной версии метода для решения практически любых реальных задач.

### 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.