Параллельные алгоритмы минимизации функционалов, ассоциированных с задачами криптографического анализа

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

Одной из наиболее интересных задач дискретной математики является задача поиска решающего набора в задаче ВЫПОЛНИМОСТЬ [1]. Перспективным направлением в построении методов решения представляется сведение КНФ к непрерывному аналогу, к задаче поиска точек глобального минимума ассоциированного функционала. В данной работе обосновывается выбор функционала специального вида и предлагается применить к решению системы нелинейных алгебраических уравнений, определяющих стационарные точки функционала, модифицированный метод последовательных приближений. В работе показано, что метод поддается распараллеливанию. Рассматривается схема применения метода к важным задачам криптографического анализа несимметричных шифров.

Введение

Область науки, носящая имя криптографический анализ в настоящее время, имеет громадное практическое значение, так как гарантированно стойкие алгоритмы шифрования являются основой надежности современных систем телекоммуникаций и систем финансовых взаиморасчетов. С теоретической стороны, прогресс в области криптографического анализа сопровождается бурным развитием смежных областей математики: алгебры, теории чисел, дискретной математики. Общие методы криптографического анализа шифров можно подразделить на две категории, одни возникли в результате исследований конкретных шифров, точнее даже стандартов: DES, ГОСТ, AES и конкретных ситуаций, связанных с вероятностью генерации слабых или связанных ключей, другие же представляют собой «интервенцию» со стороны других разделов математики, алгебры, логики, дискретной и непрерывной математики. Так, при исследовании стандарта DES были разработаны такие общие методы криптографический анализа блочных шифров, как дифференциальный криптографический анализ [2], линейный криптоанализ и метод дифференциальных искажений [3]. Применительно к AES создателями алгоритма была разработана специфическая Saturation attack [4]. Интерполяционная атака [5] и метод квадратичных уравнений [6] уже имеют более общую математическую природу и здесь возможно применить богатый арсенал дискретной математики. Основным подходом проверки криптографической стойкости асимметричных шифров в настоящее время являются алгоритмы числового решета в поле чисел общего вида [7] и различные модификации алгоритмов ρ- и λ- Полларда, основывающиеся на детерминированном случайном блуждании по группе [8], т.е. методы требуют привлечения обширного математического аппарата, хотя они и в практических реализациях специфичны. Сообщения появляющиеся время от времени лишь подтверждают стойкость известных алгоритмов. Например, для факторизации чисел «рабочих» размерностей (~1000 бит) требуется задействовать на несколько месяцев вычислительные мощности кластеров из самых верхних позиций списка Топ-500. Т.е. увеличение длины ключа в полтора или два раза решает вопрос о криптографической стойкости принципиально.

Совершенно новой альтернативой алгебраическому подходу является так называемый логический криптографический анализ, когда криптографический алгоритм, рассматривается, как программа для машины Тьюринга и подстановка открытого и шифрованного текстов в эту программу естественным образом приводит к задаче ВЫПОЛНИМОСТЬ для конъюнктивной нормальной формы. Часть выполняющего набора является ключом алгоритма. Идея такого подхода была впервые предложена в работе [9], при поиске сложных задач для тестирования решателей КНФ. Ряд исследователей, как за рубежом, так и у нас успешно работают в рамках

данного подхода [10-12]. В настоящее время проверена криптографическая стойкость ряда криптографических датчиков псевдослучайных чисел и проведены исследования стойкости нескольких раундов алгоритмов DES и ГОСТ. Как показал опыт, применение переборных алгоритмов, с частью из которых можно ознакомиться в обзоре [13], сталкивается с принципиальными трудностями, задачи криптографии оказываются действительно трудными для переборных алгоритмов, так же как задачи ВЫПОЛНИМОСТЬ для КНФ, ассоциированных со случайными системами уравнений. Естественно возникает идея перехода к непрерывным моделям, когда поиск выполнимого набора для КНФ осуществляется как поиск минимума ассоциированного с КНФ функционала. Впервые эта идея была реализована в работах [14] и [15]. Были предприняты попытки связать задачу минимизации с некой физической моделью, так в работе [16] была предложена модель химической кинетики, а в работе [17] гравитационная аналогия. Обратим внимание на то, что хотя существенных успехов на данный момент еще нет, но имеется принципиальное отличие непрерывных методов от переборных алгоритмов локального поиска, - сдвиг по антиградиенту происходит по всем переменным сразу. Так же, априори известно, что глобальный минимум функционала единственен и в случае, когда локальных минимумов и других особых точек нет, минимизация происходит эффективно. С другой стороны, достаточно очевидно, что нет необходимости в том, чтобы «точно» определить все биты ключа. Достаточно той информации, что набор бит, или ключа, или множества бит, однозначно определяющего ключ, совпадает с точным решением с вероятностью значимо большей, чем 0.5. А в результате применения итерационных методов можно надеяться на то, что мы сможем «подобраться» к такой окрестности достаточно близко. Таким образом, проверка известных в настоящее время алгоритмов на стойкость к поиску глобального экстремума является новым и необходимым тестом.

Можно надеяться, что привлечение богатого арсенала вычислительной математики к данному классу задач и синтез с методами присущими для дискретного подхода, позволит получить новые результаты и уточнит пределы применимости существующих в настоящее время криптографических алгоритмов.

1. Переход от КНФ к ассоциированным функционалам.

Пусть дана КНФ на множестве булевых переменных $y \in B^N \{0,1\}$:

$L(y) = \wedge_{i=1}^{M} c_i(y)$, где $c_i(y) = \vee_{j\in(1,\ldots,N)} l(y_j)$. Здесь $l(y_j) = y_j$ или $\bar{y}_j$.

Введем вещественные переменные $x \in R^N[0,1]$ такие, что x соответствует булевой переменной y, а $(1-x)^2$ соответствует ее отрицанию.

Рассмотрим переход от задачи ВЫПОЛНИМОСТЬ (SAT) к задаче поиска глобального минимума функционала вида (1):

$$\min_{x\in R^N[0,1]} F(x) = \sum_{i=1}^{M} C_i(x), \text{ где}$$

$$C_i(x) = \prod_{j=1}^{N} Q_{i,j}(x_j), \text{ где } Q_{i,j}(x_j) = \begin{cases} x_j^2, & \text{если } \bar{y}_j \in c_i(x) \\ (1-x_j)^2, & \text{если } y_j \in c_i(x) \\ 1, & \text{иначе} \end{cases} \qquad (1)$$

Суммирование ведется по всем M конъюнктам ДНФ, эквивалентной исходной КНФ. Переход от булевой формулы к вещественной основан на использовании соответствия:

$$\begin{cases} y_i \vee y_j \to x_i + x_j \\ y_i \wedge y_j \to x_i^2 x_j^2 \\ \bar{y}_i \to (1-x_i) \end{cases}, \text{ где } \{y_i \in B, x_i \in R\}$$

Легко заметить, что $\min\limits_{x\in R^N[0,1]} F(x)=0$ соответствует достижению значения ИСТИНА на исходной КНФ. Без потери общности можно рассмотреть 3-ДНФ, эквивалентную исходной КНФ:

$$J(x)=\sum_{\xi} z_i^2 z_j^2 z_k^2 \text{ , где } z_i=\begin{cases} x_i, & \text{если } \bar{y}_i\in c_i(y) \\ (1-x_i), & \text{если } y_i\in c_i(y) \end{cases}, \text{ здесь } c_i(x)-i \text{ триплет} \qquad (2)$$

Дифференцируя функционал по всем переменным x_i, получим систему уравнений:

$$\sum_{\xi\in\Xi} z_j^2 z_k^2 x_i=\sum_{\xi\in\Lambda} z_j^2 z_k^2,\ i=1,2,..P \text{ , где } \begin{matrix} \Xi=\{\xi, i\in\xi : x_i\in c_i(x)\} \\ \Lambda=\{\xi, i\in\xi : \overline{x_i}\in c_i(x)\} \end{matrix}, \qquad (3)$$

или $A_i(x_1\dots x_{i-1}, x_{i+1}\dots x_n)\cdot x_i = B_i(x_1\dots x_{i-1}, x_{i+1}\dots x_n),\ i=1\dots P$.

Коэффициенты A_i и B_i связаны соотношением: $A_i(x_1\dots x_{i-1}, x_{i+1}\dots x_n)\ge B_i(x_1\dots x_{i-1}, x_{i+1}\dots x_n)$.

Поясним выбор представления исходной КНФ именно в виде эквивалентной 3-ДНФ. Дифференцируя функционал $F(x)$ (1) по всем переменным x_i, получим систему уравнений аналогичную (3) при этом количество «вкладов» в A_i и B_i определятся длиной скобок (количеством литералов в исходном конъюнкте). Любая процедура решения этой системы при произвольной длине скобок естественным образом приводит к большим ошибкам округления. Ограничивая число переменных в скобках, можно исключить эту техническую трудность.

Рассмотрим систему (3), как нелинейное операторное уравнение:

$$\Phi(x)=0 \qquad (4)$$

Как показано в [18] применение метода Ньютона к решению данного уравнения неэффективно, т.к. решение принадлежит ядру производного оператора. Как альтернатива был предложен метод последовательных приближений с «инерцией» [19]:

$$\left[\sum_{p=0}^{K}\sum_{\xi\in\Xi}\alpha_k x_i(t-p)^2 x_j(t-k)^2\right]\cdot x_k(t+1)=\sum_{\xi\in\Lambda} x_j^2(t)x_k^2(t)\sim A\cdot x_i(t+1)=B$$
$$\sum_{p=1}^{K}\alpha_p=1,\ \alpha_p\in R[0,1] \qquad (5)$$

Имеется ввиду то, что итерации выполняются для вещественных чисел, а итоговый или промежуточный вектор проектируется на $B^N\{0,1\}$, и уже на булевом векторе проверяется SAT.

Ниже описаны различные модификации метода последовательных приближений с «инерцией» в применении к решению задачи K-SAT. Показаны способы повышения эффективности алгоритма при однопроцессорной и многопроцессорной реализациях алгоритма.

2. Гибридизация алгоритма.

Исходная КНФ преобразуется методом резолюции [20], что позволяет получить эквивалентную КНФ с меньшим количеством дизъюнктов и литералов.

Основная процедура состоит из последовательных итераций, которые совмещают метод последовательных приближений и сдвиг по градиенту, т.к. правая часть (3) это хотя и градиент исходного функционала, но решения (3) это всего лишь стационарные точки функционала. Например, если генерировать КНФ по заданной строке бит, случайно строя скобки, так, чтобы строка бит была решающим набором итоговой КНФ, то представительство литералов и их отрицаний будет одинаковым. Это означает, что ассоциированный функционал имеет стационарную точку, или точнее «квазистационарную» точку, с координатами 0.5 для каждой переменной т.к. $A_i\sim 2B_i$. В случае же когда представительство литералов неравное, то подобные квазистационарные точки могут быть произвольными. Например, генерируя случайную систему уравнений и сводя задачу к поиску решающего набора КНФ, мы получаем уже существенно неравное представительство литералов. В этом случае квазистационарным точкам будут соответствовать решения неопределенных систем, получаемые из исходной

системы исключением всего нескольких уравнений. Число таких точек растет экспоненциально с ростом размерности системы, и итерационная процедура поиска стационарной точки интересующей нас, как отвечающей точке минимума, практически перестает сходиться, что и подтверждается экспериментально.

Итерация состоит из двух блоков. Первый блок, определяется формулой (5), используется схема Зейделя. Второй блок – реализация сдвига по градиенту. Рассмотрим (4). Пусть $x(t)$ является решением, тогда $\Phi(x(t)) = 0$. Уравнение (5) переписывается в виде $A(x(t)) \cdot x(t) - B(x(t)) = 0$. Это необходимое условие, которому должен удовлетворять вектор решения. Если текущее *t*–е приближение не является решением, то $A(x(t)) \cdot x(t) - B(x(t)) = p$. Для итеративной формулы: $A(x(t)) \cdot x(t+1) - B(x(t)) = p$. Следовательно, что бы удовлетворить необходимому условию, необходимо перейти к вектору:

$x(t+1) = x(t) + p / A$

При приближении к решению скорость сходимости может сильно уменьшаться, одна из возможных причин этого в том, что траектория, образованная последовательными приближениями, может «зацикливатся» в областях локальных минимумов функционала. Метод смены траектории [18] позволяет выйти из локального минимума, с помощью формирования нового вектора приближения, который бы обладал свойствами не худшими, чем текущий вектор приближения, но позволял бы продолжить поиск решения.

3. Способы распараллеливания алгоритма.

Гибридный алгоритм допускает целый набор способов распараллеливания. Исходная формула, делится на определенное количество независимых частей (подформул). Для каждой подформулы находится вектор решения. Найденные вектора некоторым образом объединяются в один, который потом используется для поиска решения всей формулы. Были исследованы два способа реализации параллельного алгоритма.

3.1 Процедура 1.

ДНФ, эквивалентная исходной КНФ делится на *n* подформул. Для каждой из подформул, с помощью основного алгоритма, ищется выполнимый набор. Полученные вектора используются в качестве инициализирующего набора для следующей подформулы. После *n-1* итерации вычисляется усредненный набор. Данный набор используется в качестве инициализирующего для итерационной процедуры, которая применяется ко всей формуле. Вычислительные эксперименты показали что, выполнимый набор для подформул, состоящих из 90% (и более) от исходного числа скобок находится во всех случаях и за минимальное количество итераций (не более 20). Данный способ показал неплохие в среднем результаты при решении различных типов примеров.

3.2 Процедура 2.

ДНФ, эквивалентная исходной КНФ делится на две подформулы. Ищется выполнимый набор для каждой из двух подформул. Вычислительные эксперименты показали, что в полученных наборах решений значения литералов совпадают на 60%. Далее осуществляется формирование нового набора компонент вектора приближений для итерационной схемы путём усреднения значений переменных двух наборов, полученных на предыдущем этапе: $x_i = (x_{1i} + x_{2i}) / 2$.

Далее запускается основная схема решений, но уже для функционала, ассоциированного со всей формулой. Тесты показали, что данная процедура увеличивает число выполнимых скобок, но не всегда находит выполнимый набор для всей формулы. Для улучшения результатов была рассмотрена следующая естественная модификация. Каждый вектор решений для соответствующей подформулы, определяет точку в *n*-мерном пространстве. Между

полученными точками проводится отрезок прямой. Двигаясь по этой прямой с некоторым шагом l вычисляются новые вектора $\{x_l\}$ по формуле:

$$x_{li} = \min(x_{1i}, x_{2i}) + \frac{|x_{1i} - x_{2i}|}{k} l .$$

Для каждого набора $\{x_l\}$ вычисляется значение функционала. Затем выбирается тот набор значений $\{x_l\}$, при котором значение данного функционала минимально. Этот вектор и будет являться новым начальным набором приближений для итерационной процедуры, которая запускается для функционала, ассоциированного со всей формулой. Как показали тесты, данная процедура наиболее эффективно находит набор решений для многих тестовых формул. Конечно, есть примеры [21], для которых данный метод не вычисляет точного набора значений. Но описанная процедура позволяет максимально приблизиться к решению. В формуле остаётся до 2% скобок невыполнимыми. При этом около 2.5% переменных остаются неопределенными, то есть независимо от того какое значение они будут принимать, выполнимые скобки будут по-прежнему принимать значение ИСТИНА.

4. Результаты численных экспериментов.

После каждой модификации проводилось тестирование алгоритма для определения эффективности проделанных изменений. При тестировании использовалось несколько типов примеров: тесты с соревнований решателей SAT 2005 года [22], тесты библиотеки SATLib [23], тесты, сформированные для задачи факторизации, тесты больших размерностей, сформированные случайным образом.

4.1 Результат применения метода резолюции.

Вычислительные эксперименты показали ускорение сходимости предлагаемого метода на преобразованных методом резолюции формулах. В таблице 1 приведены результаты преобразования КНФ, ассоциированных с задачей факторизации, методом резолюции с глубиной рекурсии 1.

Таблица 1 Результат применения метода резолюции к КНФ, эквивалентным задаче факторизации.

Размерность (бит)	64	128	256	512	640	768	896	1024
Число разрешенных переменных	61	115	243	225	597	324	403	538
Число дизъюнктов до резолюции	59517	245985	999841	4031261	6308833	9094301	12387681	16188957
Число дизъюнктов после резолюции	24374	103719	426908	1743673	2731664	3941436	5339130	6977492

4.2 Метод последовательных приближений с инерцией.

Основной результат вычислительных экспериментов относительно модифицированного метода последовательных приближений, проводившихся для случайного наполнения наборов скобок SAT и 3-SAT, представлен в [18]. При соотношении $N/M \le 0.5$, где N - это число переменных, M - число скобок в 3-SAT (вплоть до $N = 10^6, M = 2 \cdot 10^6$), итерационная процедура всегда сходится к решению.

4.3 Метод последовательных приближений с инерцией (+ Сдвиг по градиенту).

Сдвиг по градиенту улучшает сходимость алгоритма. Вычислительные эксперименты со случайными формулами показали заметное уменьшение времени решения тестов. Число решенных примеров увеличилось примерно на 20%. Применение исключительно только данного приема позволило достаточно эффективно решать тестовые задачи из библиотеки SATLib, например, для КНФ серии UF20-91 удалось решить 703 теста из 1000.

4.4 Метод последовательных приближений с инерцией (+ Метод смены траектории).

Метод смены траектории существенно улучшает сходимость алгоритма. Результаты для тестовых задач различных серий из библиотеки SATLib представлены в таблице:

Таблица 2 Результаты тестирования алгоритма + метод смены траектории.

Наименование теста	Количество литералов (N)	Количество скобок (M)	Число тестов	% решенных тестов	Максимальное число итераций
Backbone-minimal Sub-instances (формулы с минимальным хребтом), 3-SAT					
RTI BMS	100 100	429 <429	500 500	98,6 79,8	19988 29831
Controlled Backbone Size Instances (формулы с хребтом фиксированного размера, b), 3-SAT					
CBS_b10 CBS_b10 CBS_b90	100 100 100	403 449 449	1000 1000 1000	100 100 98	38972 38880 29738
Uniform Random 3-SAT (UF)					
UF20-91 UF250-1065	20 250	91 1065	1000 100	100 98	448 9731
Задачи, ассоциированные с оптимизационным вариантом задачи «раскраска графа»					
FLAT30-60	90	300	100	100	4317

4.5 Увеличение разрядности вычислений.

Была исследована сходимость алгоритма при увеличении разрядности вычислений. Испытания с типами DOUBLE и FLOAT показали преимущество вычислений с двойной точностью. При переходе на тип DOUBLE количество решенных примеров увеличивается на 10%, скорость сходимости в среднем также увеличивается. Дальнейшее увеличение разрядности к значимому эффекту не приводит.

4.6 Параллельный алгоритм.

Результаты тестирования параллельных версий алгоритма на задачах из библиотеки SATLib и задачах, представленных на соревнованиях решателей SAT 2005 года приведены в таблицах 2, 3.

Таблица 3 Результаты тестирования параллельного алгоритма (Процедура 1).

Наименование теста	Количество литералов (N)	Количество скобок (M)	% решенных тестов	Максимальное число итераций
RTI BMS	100 100	429 <429	85 85	14 14
sat05-1663	2000	8400	55	200

sat05-1676 sat05-1656	4000 12000	16800 50400	50 50	200 200
UF20-91 UF250-1065	20 250	91 1065	90 90	14 21

Таблица 4 Результаты тестирования параллельного алгоритма (Процедура 2).

Наименование теста	Количество литералов (N)	Количество скобок (M)	% решенных тестов	Число итераций (часть формулы)	Число итераций (вся формула)
RTI BMS	100 100	429 <429	100 100	10 7	14 14
sat05-1663 sat05-1676 sat05-1656	2000 4000 12000	8400 16800 50400	99 99 99	20 20 20	200 200 200
UF20-91 UF250-1065	20 250	91 1065	100 100	10 20	14 21

5 Применение метода к криптографическому анализу асимметричных шифров, сводка результатов.

Приведенные выше алгоритмы, были применены для решения задач криптографического анализа. Конъюнктивные нормальные формы, ассоциированные с задачами факторизации, дискретного логарифмирования и дискретного логарифмирования на эллиптической кривой были разработаны в работах [24], [25]. Оценка роста числа дизъюнктов и скобок в зависимости от длины входа N дает нам величину $CN^2, C \approx 10$ для задачи факторизации и $C_1 N^3, C_2 N^3, C_1 \approx 100, C_2 \approx 1000$ для задач дискретного логарифмирования и дискретного логарифмирования на эллиптической кривой. Результаты применения метода резолюций к КНФ факторизации приведены выше, а применение метода резолюций к задаче дискретного логарифмирования позволяет снизить число переменных на два порядка, что приводит к относительно приемлемым цифрам для массива данных.

Для задачи факторизации получен, как представляется нам важный, результат. Уже после нескольких тысяч итераций при решении системы нелинейных уравнений (3) метод позволяет находить более 65% неизвестных. Причем, следует отметить, что найденные переменные являются ключевыми для решения задачи, т.е. после подстановки их верных значений в исходную КНФ, формула оказывается легко разрешимой относительно оставшихся переменных. Отметим, что переменными являются, биты переносов и биты, получающиеся в матрице умножения сложением строк (умножение столбиком). На рисунке 1 показаны результаты роста среднего и максимального числа верно определенных бит при увеличении длины ключа. На рисунке 2 показаны результаты роста бит для трех примеров с различной (большой) длиной ключа. На данных рисунках представлены результаты для специально отобранных «наихудших» примеров.

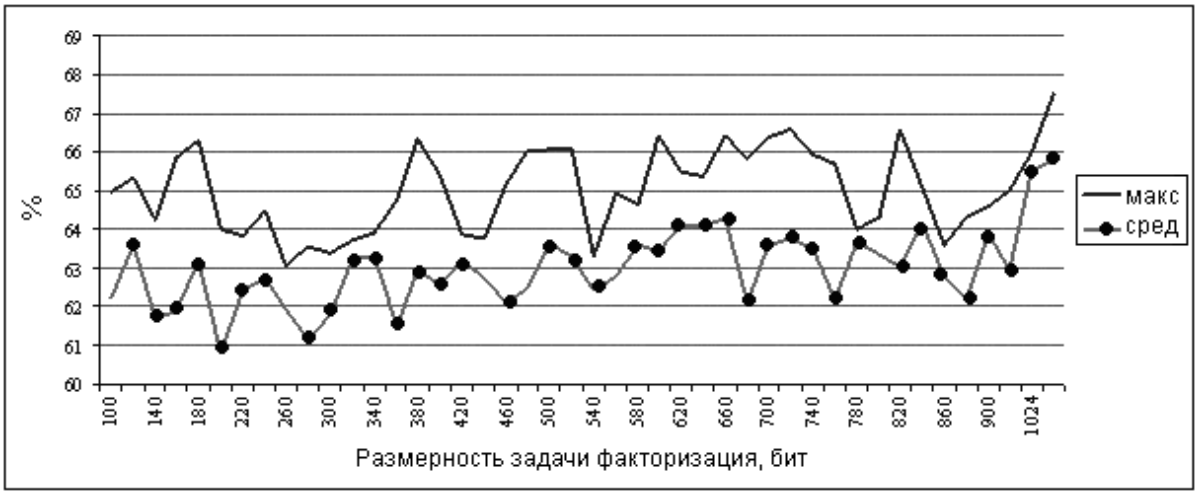

Рис. 1 Максимальный (макс) и средний (сред) процент совпадения вектора приближения с вектором решения для задачи факторизации в зависимости от размерности задачи в наихудшем случае. Результаты приведены для групп по 50 примеров для каждой из размерностей 2 e7 … 2 e10.

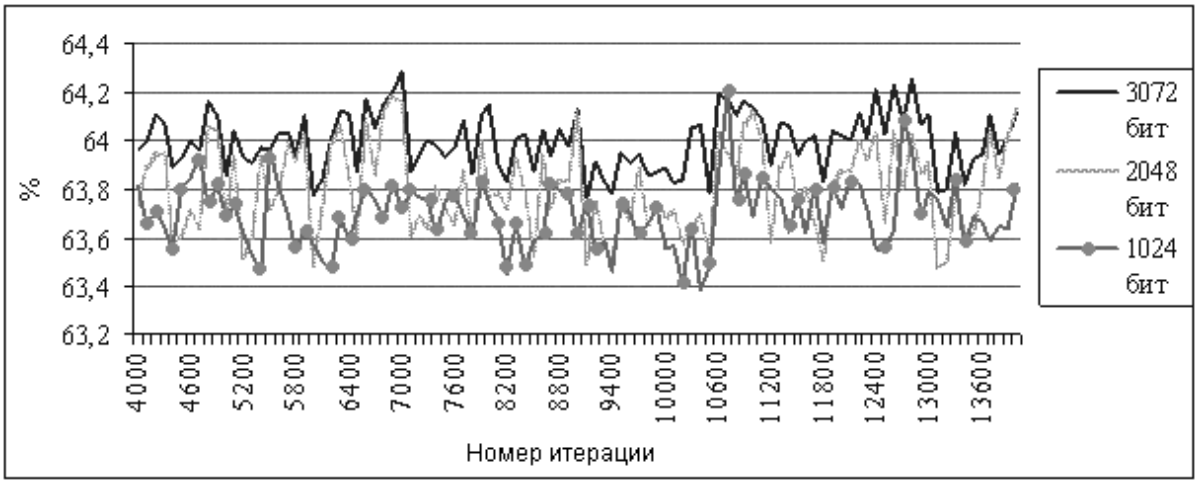

Рис. 2 Средний процент совпадения текущего вектора приближения с вектором решения для задачи факторизации в зависимости от итерации метода последовательных приближений с «инерцией» в наихудшем случае. Результаты приведены для групп по 30 примеров для каждой из размерностей 1024, 2048, 3072 бит.

Специально разработанная система тестов позволяет с высокой степенью вероятности определять биты непосредственно сомножителей. Например, таким тестом может служить проверка очевидного обстоятельства кластеризации ненулевых строк в матрице умножения при умножении в двоичной системе счисления числа p на бит числа q. Т.е. результатом будет или нулевая строка, или строка, состоящая из бит числа p. Аналогично, столбец матрицы умножения будет или нулевым столбцом, или столбцом, в котором записано число q. Отметим, что так как неизвестными являются биты ключа, биты сумм двух произвольно выбранных строк в матрице умножения и биты переноса для этих сумм, то это позволяет построить еще несколько очевидных тестов для определения бит ключа. В таблице 5 показана вероятность верного определения для 20 примеров после применения нескольких подобных тестов (при размерности чисел сомножителей 256 бит). Таким образом, для задачи факторизации числа длиной 512 бит с вероятностью большей или равной 0.8 определяются биты 13, 46, 73, 86, 101,142, 217, 255 каждого из сомножителей.

Таблица 5 Результаты численных экспериментов по определению наиболее вероятных бит в сомножителях.

Число совпадений с точным решением в 20 тестах	Частота совпадения в процентах, %	Количество совпавших бит	Доля совпавших бит в процентах от общего числа неизвестных бит (от 512 бит сомножителей)
20	100	3	0,6
17	85	1	0,2
16	80	7	1,4
15	75	20	3,9
14	70	50	9,8
13	65	83	16,2
12	60	110	21,5

Полученные результаты ставят под сомнение криптографическую стойкость алгоритма RSA, т.к. распараллеливание по вариантам и выбор тех вариантов расстановки нулей и единиц в позиции 13, 46,.., при которых значение функционала минимально, позволяет практически точно определять биты сомножителей с номерами 13, 46, ...

Литература

1. Cook S.A. The complexity of theorem proving procedures // Proceedings of the Third Annual ACM Symposium on Theory of Computing. - 1971. - P.151-158.

2. Biham E., Shamir A. Differential cryptoanalysis of DES-like cryptosystems // Proceeding of Crypto'90, Lecture Notes of CS. -1991. - P. 2-21.2. Matsui M. Linear cryptanalysis for DES Cipher // Proceedings of Eurocrypt'93, Lecture Notes of Computer Science 1994.-V.765.- P. 386-397.

3. Biham E., Shamir A. Differential Fault Analysis of Secret Key Cryptosystems // Proceeding of Crypto'97, Lecture Notes of CS. -1997. - P. 513-525.

4. Daemon J., Knudsen L., Rijmen V. The block cipher Square // Proceedings of Fast Software Encryption'97, Lecture Notes of CS. - 1997.- V. 1267. - P. 149-165.

5. Jakobsen T., Knudsen L. The interpolation attack on block cipher // Proceedings of Fast Software Encryption'97, Lecture Notes of CS. - 1997.- V. 1267. - P. 28-40.

6. Courtois N., Pipzyk J. Cryptanalysis of block ciphers with overdefined systems of equations // Proceedings Asiacrypt'02, Lecture Notes of CS. - 2002. - V.2501. -P. 267-287.

7. Lenstra A., Lenstra H. The Development of the Number Field Sieve.Springer-Verlag, 1993.

8. Koblitz N., Menezes A., Vanstone S. The state of elliptic curve cryptography. Designs Codes and Cryptography, 19, 173-193, 2000.

9. Cook S.A., Mitchel D.G. Finding hard instances for the satisfiability problem: A survey. DIMACS series in discrete mathematics and theoretical computer science. V. 5. 1997.

10. Marraro L., Massacci F. A new challenge for automated reasoning: Verification and cryptoanalysis for cryptographic algorithms -Technical Report 05-99, Dipartamento di Informatica e Sisteistica, Universita di Roma "La Sapienza", 1999.

11. Беспалов Е.В., Семенов А.А. О логических выражениях для задачи 2-ФАКТОРИЗАЦИЯ // Вычислительные технологии. -2002.- Т.7.-Ч.-2.-С. 18-25.

12. Семенов А.А., Буранов Е.Д. Погружение задачи криптоанализа симметричных шифров в пропозициональную логику // Вычислительные технологии. -2003.- Т.8. - С. 118-126.

13. Gu J., Purdom P.W.,Franco J., Wah B.W. Algorithms for the satisfiability (sat) problem / Eds. Ding-Zhu Du Jun Gu and Panos Pardalos. - Satisfiability Problem. Theory and Applications. P. 19-152. DIMACS Series in Discrete Mathematics and Theoretical Computer Science.- AMS, 1997.

14. Маслов С. Ю. Итеративные методы в переборной модели, как модель интуитивных // Тезисы IX Всесоюзной конференции по кибернетике, 1981. - С. 26-28.

15. Крейнович В.Я. Семантика итеративного метода С.Ю. Маслова //Вопросы кибернетики. Проблемы сокращения перебора.- М.: АН. СССР, 1987. -С. 30-62.

16. Матиясевич В.Ю. Возможные нетрадиционные методы установления выполнимости пропозициональных формул // Вопросы кибернетики. Проблемы сокращения перебора.- М.: АН СССР. 1987. - С. 87-90.

17. Опарин Г.А., Новопашин А.П. Непрерывные модели решения систем булевых уравнений. // Вестник Томского государственного университета №9 (1) 2004. - С. 20-25.

18. Дулькейт В.И., Файзуллин Р.Т., Хныкин И.Г. Минимизация функционалов, ассоциированных с задачами криптографического анализа // Дифференциальные уравнения. Функциональные пространства. Теория приближений. Тез. докл. Международная конференция, посвященная 100-летию со дня рождения С.Л. Соболева. - Новосибирск: Ин-т математики СО РАН, 2008. - С.484-485.

19. Файзуллин Р.Т. О решении нелинейных алгебраических систем гидравлики // Сибирский журнал индустриальной математики. -1999.-№2. -С. 176-184.

20. Хныкин И.Г. Модификации КНФ, эквивалентным задачам криптоанализа асимметричных шифров методом резолюции // Информационные технологии моделирования и управления. - 2007. №2. - С.328-337.

21. www.lri.fr/~simon/contest05/results/showbenchset-static-0-random.html

22. www.lri.fr/~simon/

23. www.satlive.org

24. 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.

25. Дулькейт В.И. КНФ представления для задачи логарифмирования на эллиптической кривой. ПРОБЛЕМЫ ТЕОРЕТИЧЕСКОЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ: Труды 39-й Всероссийской молодежной конференции. Екатеринбург: УрО РАН, 2008. - С. 360-364.