УДК 519.62.(075.8)

Сложность в криптографических системах

А.Н. Гамова
НИУ СГУ им. Н.Г. Чернышевского, г. Саратов

Теория сложности играет ведущую роль в криптосистемах, как с секретным, так и с открытым ключом. В теоретико-числовой теории сложности различают два класса – P и NP, содержащие проблемы, решаемые за полиномиальное время, соответственно, детерминированными и недетерминированными машинами Тьюринга.

В криптографических приложениях нам потребуется еще понятие вероятностной (рандомизированной) машины Тьюринга, следующий шаг которой зависит не только от состояния и обозреваемого символа, а также от случайной величины, принимающей значения 0 и 1 с вероятностью 1/2. Криптосистема (с секретным ключом K) считается стойкой, если для любой полиномиальной вероятностной машины Тьюринга M, для любого полинома $p(n)$, для достаточно больших n, имеем вероятность для криптограммы d

$$\Pr\{M(d) = (i, \sigma)\& \ \sigma = m_i : K \in_R \{0,1\}^n \& m \in_R \{0,1\}^{q(n)}\} < 1/2 + 1/p(n),$$

определяемую случайным выбором секретного ключа K, случайным выбором открытого текста m из множества всех двоичных строк длины $q(n)$, случайными величинами, используемыми машиной M.

Криптографическая стойкость системы складывается из

– вычислительной сложности задачи, положенной в основание криптосистемы, которая должна быть массовой;

– объема вычислений, который можно считать практически неосуществимым;

– вероятности, которую можно считать пренебрежительно малой (в криптографии, это Pr < 1/p(n) для всех полиномов p(n) и всех достаточно больших n, где n – длина входа).

Теоретико-сложностной подход к сложности в криптографии

Гипотеза P≠NP. Первый вопрос, возникающий при построении криптосистемы, является ли гипотеза P≠NP необходимым и достаточным условием для существования стойких криптосистем. Пусть имеется стойкая криптосистема, заданная как язык

$L = \{(K, d, i): \exists m$ – сообщение (открытый текст)$E_K(m) = d \ \& \ m_i = 1\}$, где K – (секретный) ключ, E_K - полиномиальный детерминированный алгоритм шифрования, m_i – i-ый бит сообщения.

В предположении, что P=NP, перебирая слова длины n, равной длине сообщения, можно проверить условие $E_K(m) = d \ \& \ m_i = 1$ за полиномиальное время. Что доказывает, что криптосистема нестойкая. Таким образом, гипотеза P≠NP есть необходимое условие стойкости криптосистем.

При допущении, что P≠NP, очевидно, что для построения криптосистем надо брать труднорешаемые проблемы из класса NP(NP- полные). Но поскольку в оценках сложности классов заложен наихудший вариант и они носят асимптотический характер, содержащиеся в них константы могут быть столь велики, что для менее сложных систем для некоторых входов могут быть хуже, чем для более сложных. Для криптографической стойкости нужна сложность «почти всюду». Таким образом, условие P≠NP не является достаточным для криптографической стойкости систем и необходимо искать другие дополнтельные условия.

Односторонняя функция. Определим односторонние функции $f_n : \Sigma^n \to \Sigma^m$, где $m=m(n)$, как полиномиально вычислимые функции, для инвертирования которых не существует полиномиальных алгоритмов: $\forall M \ \forall x \ \forall p(n) \ \Pr\{f(M(f(x))) = f(x)\} < 1 / p(n)$, где M – полиномиальная вероятностная машина Тьюринга, x – случайно выбранная величина (вход длины n), $p(n)$ – полином.

Из предположения о существовании односторонних функций следует гипотеза P≠NP. Однако из условия P≠NP не следует, что односторонние функции существуют.

Теорема. Существование односторонних функций есть н.и д. условие криптографической стойкости симметричных криптосистем, а также некоторых типов асимметричных криптосистем.

Для стойкости других криптосистем с открытым ключом требуются более сильные условия.

Псевдослучайные генераторы. Псевдослучайным генератором называется функция $g:\{0, 1\}^n \to \{0, 1\}^{q(n)}$, такая, что вырабатываемая ею последовательность неотличима никаким полиномиальным вероятностным алгоритмом от случайных последовательностей той же длины.

Теорема. Псевдослучайные генераторы существуют тогда и только тогда, когда существуют односторонние функции.

При анализе стойкости криптосистемы приходится использовать два подхода: теоретико-сложностной и теоретико-числовой. Последний исходит из сложности конкретной числовой задачи.

Теоретико-числовой подход к сложности в криптографии

Построение публичных ключей требует быстрого нахождения больших простых чисел. Вероятность, что n-битовое число простое, равна $1/n$. Имея полиномиальный по времени алгоритм проверки простоты числа n, мы могли бы, выбирая числа случайно, проверять их и останавливаться, обнаружив простое число. Это давало бы нам полиномиальный алгоритм типа Лас-Вегас(ZPP). К сожалению, такого алгоритма проверки на простоту нет, хотя и существует полиномиальный алгоритм типа Монте-Карло (RP).

Безопасность шифрования многих криптосистем зависит от невозможности разложить произвольное целое число на простые множители за полиномиальное время. Если бы оказалось, что множество простых или множество составных чисел образует NP-полный класс, тогда полиномиальный алгоритм разложения числа на простые множители доказывал бы равенство P = NP, что маловероятно. С другой стороны, будет доказано, что оба языка (простых и составных чисел) принадлежат NP. Они дополняют друг друга, поэтому, если бы какой-то из них был NP-полным, то NP = co-NP, что также вызывает сомнение. Кроме того, ввиду принадлежности языка простых чисел классу RP, NP-полнота последнего влекла бы равенство RP = NP, которое также маловероятно.

Рандомизированная полиномиальная проверка простоты. Опи- шем, как применять рандомизированные алгоритмы для поиска боль- ших простых чисел. Полиномиальная рандомизированная машина Тьюринга типа Монте-Карло имеет не менее 50% шансов на допускание своего входа, если вход принадлежит языку LєRP. Покажем, что язык составных чисел принадлежит RP. Метод генерации n-битовых простых чисел состоит в следующем: случайно выбирается n-битовое число и много раз применяется алгоритм Монте-Карло для распознавания составных чисел. Если некоторая проверка показала, что число составное, то число точно не простое. Если все проверки не показывают, что число составное, то вероятность, что оно составное. не больше 2^{-k}, где k – число проверок. Т.е. с большой долей уверенности можно сказать, что число простое, и этим обосновать безопасность криптографических операций.

Идея рандомизированного алгоритма базируется на теореме Ферма: если p – простое число, то для любого x, $x^{p-1} = 1(mod\ p)$.

Рандомизированный алгоритм типа Монте-Карло для составных чисел. Если p – простое, то $x^{p-1} = 1(mod\ p)$, машина Тьюринга остановится без допускания. Это одна ветвь работы машины типа Монте-Карло: если вход не принадлежит языку, то он никогда не допускается и при повторном запускании на этом входе. Для составных чисел p не менее половины чисел x из интервала $[1, p]$ удовлетворяют неравенству $x^{p-1} \neq 1\ (mod\ p)$, здесь машина допускает. Есть однако небольшое количество нечетных составных чисел n, для которых теорема Ферма выполняется для всех x из интервала $[1,n-1]$, взаимно простых с n, они требуют еще одной, более сложной проверки на непростоту. Два условия для языков из класса RP выполнены.

Однако здесь не говорится о том, как разложить составное число на множители за полиномиальное время, по-видимому, такого, даже рандомизированного, алгоритма нет. В противном случае, криптографические методы защиты, основанные на невозможности разложить очень большие числа на простые множители за полиномиальное время оказались бы небезопасными.

Недетерминированная проверка простоты. Здесь будет доказано, что языки простых и составных чисел принадлежат NP∩co-NP. Отсюда следует, что вероятность NP-полноты этих языков ничтожна, иначе NP = co-NP, что совершенно невероятно.

Теорема. Множество составных чисел принадлежит NP.

Доказательство. Строим недетерминированный полиномиальный алгоритм распознавания составных чисел: 1) Имея n-битовое число p, угадываем сомножитель $q \neq 1, p$. 2) Если это так, то эта часть детерминирована и может быть выполнена за время $O(n^2)$ на многоленточной МТ. Эта ветвь недетерминированной МТ ведет к допусканию. 3)Наоборот, допускание НМТ означает, что найден делитель числа p, $q \neq 1, p$. Язык описанной НМТ содержит все составные числа.

Теорема. Множество простых чисел принадлежит NP.

Доказательство. Пусть p n-битовое число, не равное 1, 2, 3.

1. Угадываем список сомножителей $\{q_1,q_2,\ldots,q_k\}$, двоичные представления которых вместе занимают не более $2n$ битов, и ни одно из них не имеет более n-1 битов. На каждой ветви НМТ время работы $O(n)$.

2. Перемножаем все сомножители и проверяем, равно ли их произведение p-1. Это потребует времени не более $O(n^2)$.

3. Если произведение совпало с p-1, то рекурсивно проверим, что каждый сомножитель является простым.4)Если не все сомножители q являются простыми, угадаем значение x и проверим неравенство $x^{(p-1)/q} \neq 1$ для каждого q, делящего p-1. Тем самым устанавливается, что *ord x* равен p-1, иначе *ord x* должен делиться на один из множителей (p-1) /q, что противоречит полученному выше неравенству. Возведение в степень осуществляется эффективным алгоритмом, сделав не более k умножений ($k< n$), затратив времени $O(n^3)$, так что общее время – $O(n^4)$. Построенный недетерминированный алгоритм полиномиален вдоль каждой ветви, кроме шага 3. Рекурсивное вычисление на шаге 3, представим в виде дерева, в корне которого находится n-битовое число p, сыновьями являются угаданные сомножители числа p-1, под каждым q_i – угаданные сомножители числа q_i –1 и т.д. Таким образом, время работы на каждой ветке $O(n^5)$.

УДК 519.6

О точных решениях линейных уравнений в комплексных круговых интервалах

В.С. Дронов, Н.А. Кузнецов
АлтГУ, г. Барнаул

Несмотря на то, что расширение подхода интервального анализа с действительного случая на комплексный является давней идеей (см., например, [1]), и существует достаточно обширный класс задач, приводящих к появлению интервальной неопределённости в комплексных данных (см. в [2] примеры задач, растущих из практики, и в [3] примеры теоретических), в целом комплексные интервальные методы развиты ощутимо хуже действительных.

Одной из проблем переноса интервальных методов на комплексный случай являются свойства операций над комплексными числами, во многих случаях «ломающие» простоту действительных подходов. Во многом из-за разных взглядов на то, что в комплексных данных заслуживает интервализации, не существует и единого подхода к определению комплексного интервала. Двумя имеющими давнюю историю вариантами являются прямоугольные и круговые комплексные интервалы (естественным образом связанные с алгебраической и тригонометрической формой записи комплексного числа). Не менее естественной в этом смысле, но менее известной формой являются секторные интервалы в терминах [2]:

$$\{x \epsilon C : x = \rho e^{i\theta}, \rho \in \boldsymbol{\rho}, \theta \in \boldsymbol{\theta}\}$$

Классическим результатом для так называемого объединённого множества решений систем линейных уравнений в действительном интервальном случае является теорема Бека-Никеля, обеспечивающая возможность оценки объединённого множества решений по крайним точкам исходных интервальных данных. Из-за свойств операций над комплексными числами, прямой перенос этой теоремы на комплексный случай или прямо неверен (для прямоугольных и секторных интервалов), или существенно менее полезен из-за отсутствия порядка на комплексных числах (для круговых интервалов). В действительном случае объединённое множество решений интервальной системы линейных уравнений представляет собой «звёздчатое» множество – пересечение которого с каждым ортантом представляет собой выпуклое многогранное множество. Для комплексного случая это неверно. На рисунке 1 приводится пример из [4], где рассмотрено устройство объединённого множества решений для прямоугольных комплексных интервалов.

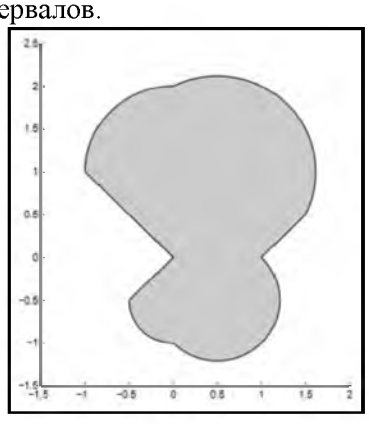

Рисунок 1 – объединённое множество решений уравнения
[1-i, 5+i]**z**=[-i, 1+2i] в прямоугольных интервалах