Редукция NP сложной задачи. Шифрование с открытым ключом.

Кренделев Сергей Федорович
Новосибирский государственный университет

ВВЕДЕНИЕ

- Начнем с известной сложной задачи. Даны: целочисленная матрица $\mathbf{A}$ размера, $\mathbf{m} \times \mathbf{n}$ элементы которой целые числа, вектор $\mathbf{b}$ размера $\mathbf{m}$, состоящий из целых чисел. Задача: разрешима ли в неотрицательных числах система
- $$\mathbf{Ax} = \mathbf{b} \qquad (1)$$
- Утверждается, что эта задача - **NP** полная. Основная стратегия, применяемая в криптографии, заключается в том, что бы построить систему уравнений (1), которая легко решается за разумное время, после чего систему уравнений преобразовать таким образом, что бы она выглядела как произвольная система уравнений вида (1). Тем самым задача дешифрования становится - **NP** полной. Типичной является задача об укладке рюкзака, которую стандартным образом преобразуют в трудную задачу. Неприятные свойства, которые позволяют осуществить вскрытие за полиномиальное время, это единственность решения, решение является минимальным вектором решетки, всякому тексту сопоставляется шифртекст единственным образом. В данной работе рассматривается подход, в котором эти свойства не имеют места.

Легко решаемые системы уравнений

- Простейшим случаем легко решаемой системы линейных уравнений является представление числа в некоторой системе счисления. Выберем некоторое число $\lambda>1$
- Рассмотрим систему уравнений
- $$a_0+a_1\lambda+a_2\lambda^2+\ldots+a_n\lambda^n=d \qquad (2)$$
  $$d<\lambda^{n+1}, 0\le a_i<\lambda \quad i=0,1,\ldots,n$$
- Очевидно, что данное уравнение имеет единственное решение, которое находится разложением числа d по известному основанию. Если ввести вектора

$$\mathbf{u}=(1,\lambda,\lambda^2,\ldots,\lambda^n),\ \mathbf{s}=(a_0,a_1,a_2,\ldots,a_n)$$

- То уравнение приобретает вид

$$(\mathbf{u},\mathbf{s})=d$$

Легко решаемые системы уравнений

- Очевидно, что последовательность $1,\lambda,\lambda^2,\ldots,\lambda^n$
- сверхвозрастающая. Однако решить уравнение (2) однозначно возможно для любой последовательности вида $1,\pm\lambda,\pm\lambda^2,\ldots,\pm\lambda^n$ где знаки расставлены произвольным образом, а эта последовательность не является сверхвозрастающей.
- Любой вариант позиционной системы счисления подходит для построения легко решаемой системы линейных уравнений. Например системы с отрицательным основанием, смешанным основанием и т.д.

Легко решаемые системы уравнений

- С помощью позиционных систем счисления строится одно уравнение, для построения систем уравнений можно использовать матричные варианты позиционных систем счисления.

Вариант 1. Обобщение вариантов позиционных систем счисления, для векторов строится следующим образом. Пусть $\mathbf{A}$ некоторая целочисленная матрица размера $k \times k$, $\mathbf{w_0}, \mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_s}$ набор векторов из модуля Z^k. Вычислим векторную сумму

$$\mathbf{u} = \mathbf{w_0} + \mathbf{A}\mathbf{w_1} + \mathbf{A}^2\mathbf{w_2} + \ldots + \mathbf{A}^s\mathbf{w_s} \quad (3)$$

Задача формулируется так, пусть задана матрица $\mathbf{A}$ и вектор $\mathbf{u}$, найти набор векторов $\mathbf{w_0}, \mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_s}$ таких, что выполнено (3). Если действовать согласно логике позиционных систем счисления, то для разложения необходимо представить (3) в виде

$$\mathbf{u} = \mathbf{w_0} + \mathbf{A}(\mathbf{w_1} + \mathbf{A}\mathbf{w_2} + \ldots + \mathbf{A}^{s-1}\mathbf{w_s})$$

Легко решаемые системы уравнений

Если обозначить

$$\mathbf{v} = \mathbf{w}_1 + \mathbf{A}\mathbf{w}_2 + \ldots + \mathbf{A}^{s-1}\mathbf{w}_s$$

То уравнение (3) приобретает вид

$$\mathbf{u} = \mathbf{w}_0 + \mathbf{A}\mathbf{v} \quad (4)$$

Тем самым задача свелась к вопросу, в каком случае система уравнений (3) имеет при заданном векторе $\mathbf{u}$ единственное решение $\mathbf{w}_0, \mathbf{v}$. Кроме того если есть единственное решение то необходимо уметь его найти. Выбор матрицы $\mathbf{A}$, для которой уравнение (3) решается однозначно может быть осуществлен, например, с помощью теории решеток. Подобные задачи возникают в системе шифрования NTRU, LWE

Легко решаемые системы уравнений

Вариант 2. Пусть $\mathbf{A}$ некоторая целочисленная матрица, у которой есть собственный вектор $\mathbf{u}$ и собственное значение матрицы для этого вектора равно λ. Собственное число считается целым. Другими словами

$$\mathbf{Au} = \lambda\mathbf{u}$$

Очевидно, что для матрицы $\mathbf{A}^k$ собственный вектор также $\mathbf{u}$, и он имеет собственное значение равное λ^k. Тем самым имеет место соотношение

$$\mathbf{A}^k\mathbf{u} = \lambda^k\mathbf{u}$$

Откуда следует, что если дана матрица $\mathbf{S}$ сумма степеней матрицы $\mathbf{A}$

$$\mathbf{S} = a_0\mathbf{A}^0 + a_1\mathbf{A}^1 + a_2\mathbf{A}^2 + \ldots + a_r\mathbf{A}^r$$

Легко решаемые системы уравнений

Имеет место соотношение

$$\mathbf{Su} = a_0\mathbf{A}^0\mathbf{u} + a_1\mathbf{A}^1\mathbf{u} + a_2\mathbf{A}^2\mathbf{u} + \ldots + a_r\mathbf{A}^r\mathbf{u} =$$

$$a_0\mathbf{u} + a_1\lambda^1\mathbf{u} + a_2\lambda^2\mathbf{u} .. + a_r\lambda^r\mathbf{u} = (a_0 + a_1\lambda^1 + a_2\lambda^2 .. + a_r\lambda^r)\mathbf{u}$$

Это равенство умножим скалярно слева и справа на вектор $\mathbf{u}$, получаем

$$(\mathbf{Su}, \mathbf{u}) = (a_0 + a_1\lambda^1 + a_2\lambda^2 .. + a_r\lambda^r)(\mathbf{u}, \mathbf{u})$$

Поскольку равенство рассматривается в целых числах, то $(\mathbf{Su}, \mathbf{u})$ делится на число $(\mathbf{u}, \mathbf{u})$. Следовательно

$$a_0 + a_1\lambda^1 + a_2\lambda^2 .. + a_r\lambda^r = d$$

где число d известно. Таким образом, получается задача, связанная с системами счисления рассмотренная выше.

Легко решаемые системы уравнений

- Подобные конструкции обобщаются очевидным образом на аналог смешанных систем счисления.
- В этом случае на каждом шаге матрица выбирается различной.

Как маскировать легко разрешимую задачу

Будем говорить, что вектор $\mathbf{u}$ восстанавливает вектор $\mathbf{s}$, если из того, что нам известно скалярное произведение $d = (\mathbf{u}, \mathbf{s})$, вектор $\mathbf{u}$ и ограничения на вектор $\mathbf{s}$ можно однозначно определить вектор $\mathbf{s}$. Соответственно будем говорить, что набор векторов $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_k}$ восстанавливает вектор $\mathbf{s}$, если из того, что нам известен набор скалярных произведений

$$d_i = (\mathbf{u}, \mathbf{s}) \quad i=1,2,\ldots,k$$

и ограничения на вектор $\mathbf{s}$, можно однозначно определить вектор $\mathbf{s}$. Примеры, приведенные выше, дают варианты построения восстанавливающих наборов векторов. Естественно все варианты можно комбинировать в разных сочетаниях.

Как маскировать легко разрешимую задачу

Очевидно, что если набор векторов $\mathbf{u_1, u_2, \ldots, u_k}$ является восстанавливающим, то для любого набора векторов $\mathbf{v_1, v_2, \ldots, v_r}$, объединение наборов $\mathbf{u_1, u_2, \ldots, u_k, v_1, v_2, \ldots, v_r}$ также является восстанавливающим.

Всякое невырожденное линейное преобразование переводит набор восстанавливающих векторов в набор восстанавливающих векторов.

Действительно, пусть дана целочисленная $k \times k$ матрица $\{a_{ij}\}$ с ненулевым определителем. Тогда определим новый набор векторов $\mathbf{w_1, w_2, \ldots, w_k}$ по правилу

$$\mathbf{w}_i = \sum_{j=1}^{k} a_{ij}\mathbf{u}_j \quad i=1,2,\ldots,k$$

Тогда

$$(\mathbf{w}_i, \mathbf{s}) = p_i = \sum_{j=1}^{k} a_{ij}(\mathbf{u}_j, \mathbf{s}) = \sum_{j=1}^{k} a_{ij} d_j ,$$

по построению уравнение

$$p_i = \sum_{j=1}^{k} a_{ij} d_j \quad i=1,2,\ldots,k$$

однозначно разрешимо в целых числах.

Как маскировать легко разрешимую задачу

Предположим, что $\mathbf{u_1, u_2, \ldots, u_k}$ восстанавливающий набор векторов. И существует набор чисел $\alpha_1, \alpha_2, \ldots, \alpha_r$ такой, что $\mathbf{u_1} = \alpha_1 \mathbf{v_1} + \alpha_2 \mathbf{v_2} + \ldots + \alpha_r \mathbf{v_r}$, тогда набор $\mathbf{u_2, \ldots, u_k, v_1, v_2, \ldots, v_r}$ является восстанавливающим.

В качестве усиления стойкости шифрования можно применять схему Меркла-Хеллмана, связанную с сильным модульным умножением. Очевидно, что параметры сильного модульного умножения для всякого вектора можно выбирать свои.

Для шифрования с открытым ключом, необходимо всем желающим сообщить набор восстанавливающих векторов $\mathbf{u_1, u_2, \ldots, u_k}$ и ограничения на компоненты вектора сообщения $\mathbf{s}$.

Игрушечный пример

- Шифровать будем битовые последовательности.
  В качестве системы счисления, выберем смешанную систему счисления с взаимно простыми основаниями. В данном случае набор m_1, m_2, m_3, m_4 выберем 3,5,7,8. Произведение этих чисел равно 850. Теперь выберем числа M_1, M_2, M_3, M_4 такие, что $M_j = 1 \bmod(m_j), M_j = 0 \bmod(m_k)\ j \neq k$
  В нашем случае это набор (280,336,120,105) . В принципе это набор можно изменить сильным модульным умножением, но этого делать не будем.
  Поскольку требуется вероятностное шифрование, то присвоим биту 0 два числа

$$2,2,3,1 \quad 2\times 280 + 2\times 336 + 3\times 120 + 1\times 105 = 17 \bmod(840)$$

$$2,1,3,4 \quad 2\times 280 + 1\times 336 + 3\times 120 + 4\times 105 = -4 \bmod(840)$$

Игрушечный пример

- Биту 1 также присвоим два числа

$$1,3,2,3 \quad 1\times 280+3\times 336+2\times 120+3\times 105=163 \bmod(840)$$

$$1,4,1,5 \quad 1\times 280+4\times 336+1\times 120+5\times 105=-251 \bmod(840)$$

- Битовому сообщению 0,1,0,1 может соответствовать число

$$17\times 280+163\times 336-4\times 120-251\times 105=$$

$$4760+54768-480-26355=-26835=32693$$

- Или число

$$-4\times 280+163\times 336-4\times 120-251\times 105=$$

$$-1120+54768-480-26355=26813$$

- Для дешифрования, например бита 3 необходимо вычислить $32693 \bmod(7)=3$ или $26813 \bmod(7)=3$ а это соответствует числу 17 или -4.

Игрушечный пример

- Маскировка восстанавливающего вектора (280,336,120,105) . Простейший вариант это разложить данный вектор по какому либо основанию. Пусть основание 37, тогда получаем два вектора

$$(21,3,9,31),(7,9,3,2)$$

Очевидно

$$37\times(7,9,3,2)+(21,3,9,31)=(280,336,120,105)$$

И следовательно данная пара векторов восстанавливающая.

Теперь будем добавлять возможность не единственности

Для этого продолжим два восстанавливающих вектора

$$\mathbf{v}_1 = (21,3,9,31,0,0,0,0)$$
$$\mathbf{v}_2 = (7,9,3,2,0,0,0,0)$$

Игрушечный пример

- Добавим два произвольных вектора

$$\mathbf{v}_3 = (2,13,9,-4,3,-11,2,-1)$$

$$\mathbf{v}_4 = (-7,5,8,-2,5,-6,-11,7)$$

- Образуем линейные комбинации из этих векторов

$$\mathbf{v}_1 + \mathbf{v}_3 = (23,16,18,27,3,-11,2,-1)$$

$$\mathbf{v}_2 + \mathbf{v}_4 = (0,14,11,0,5,-6,-11,7)$$

$$\mathbf{v}_3 + 2\mathbf{v}_4 = (-12,23,25,-8,13,-23,-20,13)$$

$$2\mathbf{v}_3 - 3\mathbf{v}_4 = (25,11,-6,-2,-9,-4,-29,-22)$$

- По построению по этим четырем векторам однозначно восстанавливается первые 4 бита восьми битового сообщения.

Игрушечный пример

- Последний шаг – сортировка векторов. Будем интерпретировать набор из 4-х векторов как матрицу размера , у которой надо отсортировать столбцы.
- Сортировка осуществляется так, чтобы в каждой паре идущей подряд была позиция не восстанавливающая и восстанавливающая. В какой последовательности не важно. Теперь этот новый набор векторов объявляется открытым ключом, передаются представления для 0,1 и сообщается, что каждая пара должна быть одинаковой. Т.е. Если в позиции есть 0, то кодируется два 0 подряд, аналогично для 1.
- Открытый ключ рассортированная четверка векторов, представления для битов 0,1 и указание как шифровать пары.

Благодарю за внимание

- **ВОПРОСЫ ?**