КРИПТОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ КАНОНИЧЕСКИХ СИСТЕМ СЧИСЛЕНИЯ

Федосеев В.А.
Самарский государственный аэрокосмический университет

В статье рассматривается криптографическая система, базирующаяся на существования позиционных систем счисления в квадратичных полях.

Введение

В работах [1, 2] введено понятие канонических систем счисления (КСС) в кольцах целых элементов квадратичных полей, позволяющих представлять элементы таких колец конечными линейными комбинациями степеней некоторого целого элемента квадратичного поля по аналогии с обычными позиционными системами счисления для целых чисел. В данной работе рассматривается приложение этой относительно новой теории к задачам криптографии.

Сформулируем основные определения и необходимые сведения из теории КСС.

Пусть $\mathbf{Q}\left(\sqrt{d}\right)$ - квадратичное поле:

$$\mathbf{Q}\left(\sqrt{d}\right)=\left\{z=a+b\sqrt{d}:a,b\in\mathbf{Q}\right\},$$

$z=a+b\sqrt{d}=\mathbf{Rat}(z)+\sqrt{d}\mathbf{Irr}(z)$, где d есть свободное от квадратов целое число.

Пусть $\mathbf{S}\left(\sqrt{d}\right)$ есть кольцо его целых элементов:

$$\mathbf{S}\left(\sqrt{d}\right)=\left\{z\in\mathbf{Q}\left(\sqrt{d}\right):\mathbf{Norm}(z)=a^2-db^2,\mathbf{Tr}(z)\in\mathbf{Z}\right\}$$

Определение 1. Целое алгебраическое число $\alpha=A+\sqrt{d}$ есть основание канонической системы счисления в кольце $\mathbf{S}\left(\sqrt{d}\right)$ целых элементов поля $\mathbf{Q}\left(\sqrt{d}\right)$ если любой элемент $z\in\mathbf{S}\left(\sqrt{d}\right)$ представляется единственным образом конечной суммой

$$z=\sum_{j=0}^{k(z)}z_j\alpha^j,$$

где «цифры» z_j принадлежат конечному подмножеству

$$\mathsf{N}=\left\{0,1,\ldots,\left|\mathbf{Norm}(\alpha)\right|-1\right\},\ \mathbf{Norm}(\alpha)=A^2-d\ .$$

В зависимости от того, является ли поле $\mathbf{Q}\left(\sqrt{d}\right)$ вещественным ($d>0$) или мнимым ($d<0$), исчерпывающее описание канонических систем счисления дано в [1, 2]. Нам потребуется частный случай существования КСС, который мы сформулируем в форме леммы.

Лемма 1. (a) *Пусть поле* $\mathbf{Q}\left(\sqrt{d}\right)$ *- вещественное,* $0<d\equiv 2,3\ (\mathrm{mod}\,4)$. *Тогда алгебраическое число* $\alpha=A\pm\sqrt{d}$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(\sqrt{d}\right)=\mathbf{Z}\left(\sqrt{d}\right)$ *тогда и только тогда, когда* $A\in\mathbf{Z}$ *и*

$$0<-2A\le A^2-d\ge 2\ .$$

(b) *Пусть поле* $\mathbf{Q}\left(\sqrt{d}\right)$ *- вещественное,* $0<d\equiv 1\,(\mathrm{mod}\,4)$. *Тогда алгебраическое число* $\alpha=\frac{1}{2}\left(B\pm\sqrt{d}\right)$ *является основанием канонической системы счисления в кольце* $\mathbf{S}\left(\sqrt{d}\right)\supset\mathbf{Z}\left(\sqrt{d}\right)$ *тогда и только тогда, когда* $B\in\mathbf{Z}$ *нечетно и*

$$0<-B\le\frac{1}{4}\left(B^2-d\right)\ge 2$$

Существует рекуррентная процедура, позволяющая находить «цифры» z_i для представления целого элемента квадратичного поля в КСС [3]

Лемма 2. Пусть целое $d\ge 2$ свободно от квадратов.

(a) Пусть $d\equiv 2,3\left(\mathrm{mod}\,4\right)$, то $\alpha=A\pm\sqrt{N}$ – базис канонической системы счисления, $z=x+y\sqrt{d}\in\mathbf{S}\left(\sqrt{d}\right)$, $N(\alpha)=\mathbf{Norm}(\alpha)=A^2-d$. Определим последовательность s_i рекуррентным соотношением:

$$s_{-1}(z)=\mp yN(\alpha),$$
$$s_0(z)=x\mp Ay,$$
$$s_{k+1}(z)=2A\left[\frac{s_k(z)}{N(\alpha)}\right]-\left[\frac{s_{k-1}(z)}{N(\alpha)}\right],k\ge 0\ .$$

(b) Пусть $d\equiv 1\left(\mathrm{mod}\,4\right)$, $\alpha=\frac{1}{2}\left(B\pm\sqrt{d}\right)$ – базис канонической системы счисления, $z=x+\frac{1+\sqrt{d}}{2}y\in\mathbf{S}\left(\sqrt{d}\right)$. Определим последовательность s_i рекуррентным соотношением:

$$s_{-1}(z)=\mp yN(\alpha)$$
$$s_0(z)=x\mp\frac{B-1}{2}y$$
$$s_{k+1}(z)=A\left[\frac{s_k(z)}{N(\alpha)}\right]-\left[\frac{s_{k-1}(z)}{N(\alpha)}\right],k\ge 0\ .$$

Тогда

$z=\sum_{k\ge 0}z_k\alpha^k$, где $z_k\equiv s_k(z)\left(\mathrm{mod}\,N(\alpha)\right)$.

Описание криптосистемы

Пусть шифротекст имеет числовой эквивалент – целое число $z = z + 0 \cdot \sqrt{d}$. Секретными ключами криптосистемы являются целые числа A, d, такие, что целое квадратичное число $\alpha = A + \sqrt{d}$ или $\alpha = \frac{1}{2}\left(A \pm \sqrt{d}\right)$ (в зависимости от вычета числа $d \pmod 4$) является основанием канонической 2^t-значной КСС (t – открытый ключ).

Если Алиса хочет послать сообщение $z = z + 0 \cdot \sqrt{d}$ Бобу, то она вычисляет в соответствии с Леммой 2 последовательность цифр z_j для представления z в КСС с основанием α. Так как каждая из цифр z_j однозначно представляется t–битовым вектором, то сообщение z преобразуется в шифротекст – битовую последовательность длины tK, где K – число цифр представления сообщения z в КСС с основанием α.

Получив сообщение, Боб выделяет из битовой последовательности t–членные блоки – обычные двоичные коды «цифр» z_j и , зная основание α, восстанавливает сообщение.

Параметры криптосистемы

При изучении криптографической системы одним из основных вопросов является выбор таких параметров A и N, при которых задача шифрования текста была бы как можно более простой, а дешифрации – как можно более сложной.

Изучим взаимосвязь параметров и ограничения, определяющие их выбор. Число N должно быть свободно от квадратов и $N \equiv 2,3 \pmod 4$. Число $A < 0$ и $|A| \le 2^{t-1}$. Также эти два параметра связаны соотношением $A^2 - N = 2^t$.

Таким образом, перед отправителем фактически ставится задача генерации числа A, удовлетворяющего следующим соотношениям:

$$A < 0, \tag{1}$$

$$2^{\left\lceil \frac{t}{2} \right\rceil} \le |A| \le 2^{t-1}, \tag{2}$$

$$A^2 - 2^t \equiv 3 \pmod 4 \tag{3}$$

и свободно от квадратов.

Такое число однозначно определяет криптосистему. При достаточно большой степени t найдется большое количество чисел, удовлетворяющих этим соотношениям, и раскрытие ключа (A,N) представляется достаточно тяжелой задачей.

Таким образом, основная задача, стоящая перед разработчиком криптосистемы, заключается в проверке большого целого числа на отсутствие квадратичных сомножителей в его каноническом разложении на простые сомножители. Это может быть сделано различными методами.

Рассмотрим отдельно случай, когда выбранное открытое число t является четным: $t = 2k$. Тогда $N = A^2 - 2^{2k} = \left(A - 2^k\right)\left(A + 2^k\right)$. Число N свободно от квадратов тогда и только тогда, когда числа $A - 2^k$ и $A + 2^k$ свободны от квадратов и взаимно просты. Взаимная простота быстро проверяется по алгоритму Евклида, а проверка на взаимную простоту этих чисел осуществляется быстрее, чем для числа N.

В отличие от разработчика, выбирающего параметры криптосистемы, взломщик вынужден проверять большое количество чисел, подчиняющихся условиям (1) – (3). В том числе и проверять на наличие квадратичных сомножителей. Априорная информация, следующая из условия (3) не облегчает задачу раскрытия ключа, которая сводится, в частности, к «трудной» вычислительной задаче факторизации целых чисел.

Устойчивость шифротекста к декодированию методом частотного анализа

Рассмотрим простейший способ приведения открытого текста к виду $z = x + y\sqrt{d} \in \mathbf{S}\left(\sqrt{d}\right)$: текст переводится кодом подстановки, в котором каждой букве соответствует ее номер в алфавите (от 0 до 31, без буквы «ё», пробелов и знаков препинания), в число z_1, а число z_2 принимается равным нулю. Таким образом, в числе $z = z_1$ каждые 5 бит соответствуют одной букве алфавита. Если в шифротексте удастся выделить битовые куски, соответствующие отдельным буквам, то взломщик при помощи частотного анализа сможет дешифровать текст. Наша задача – изучить связь последовательности битов числа z с последовательностью битов шифротекста.

В первую очередь заметим, что число бит открытого текста равно числу букв, помноженному на 5, т.е. пропорционально длине сообщения, тогда как число бит шифротекста $\le t(t+1)$, то есть, ограничено параметром кодирования, и, следовательно, не пропорционально длине сообщения. Это значит, что между последовательностями битов не существует точного соответствия. Однако определенные связи между ними все же имеют место.

Пример 1. Пусть открытый текст – “ООО”, в битовой форме 011100111001110. Шифротекст при кодировании с параметрами $A = -7$ и $t = 5$:

1001010010100101010110110001111001110000111 10

Шифротекст при кодировании с параметрами $A = -37$ и $t = 10$:

10000011110011111111010000111001110

Как видим, в обоих случаях несколько младших бит совпали с открытым текстом. Однако, и в первом, и во втором случае остаются еще большие несовпадающие битовые участки, длина которых значительно превышает длину одной буквы (что подтверждает сказанное выше о длине шифротекста).

Пример 2. Пусть открытый текст – слово «КАПКАН»:

10100000001111010100000001101

Шифротекст при кодировании с параметрами $A=-7$ и $t=5$:

10010101101100110011001000110001100010101000000000100101111010110101111000010011110100010000000000001101

Шифротекст при кодировании с параметрами $A=-37$ и $t=10$:

11111111100111001001010001101000110111111001001001101001100101110000000001101

При кодировании этого слова также совпали несколько младших бит шифра и текста, причем их количество практически не изменилось от увеличения слова. Изменяется оно при увеличении параметров кодирования (возрастает). Это явление объясняется тем, что эти биты относятся к свободному члену в канонической системе счисления, и значит равны битам исходного числа. В остальной же части шифротекста невозможно выделить отдельные буквы, следовательно, взломщик не может применить частотный анализ для декодирования текста. При большом размере шифруемого текста известность для взломщика нескольких последних букв без возможности выделения остальных не является угрожающим фактором. К тому же эти последние буквы могут не нести информацию (например, заполнение конца текста многоточиями).

Благодарности

Работа выполнена при поддержке российско-американской программы «Фундаментальные исследования и высшее образование» (BRHE).

Литература

1. Katai I., Kovacs B. Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen // Acta Sci.Math.(Szeged) 42, 1980, pp. 99–107.
2. Kátai I., Kovács B. Canonical Number Systems in Imaginary Quadratic Fields // Acta Math. Acad. Sci. Hungaricae, v.37, 1981, pp.159-164.
3. Thuswardner J.M. Elementary properties of canonical number systems in quadratic fields // Applications of Fibonacci Numbers, F.T.Howard (Editor), v. 7, Kluwer, 1998, pp.405-409.